Constrained Quantum Tomography

Michael Kech

Zentrum Mathematik M5

Technische Universität München

A thesis submitted for the degree of

Doctor rerum naturalium

August 2016

TECHNISCHE UNIVERSITÄT MÜNCHEN
ZENTRUM MATHEMATIK

Lehrstuhl für mathematische Physik

Constrained Quantum Tomography

Michael Kech

Vollständiger Abdruck der von der Fakultät für Mathematik der Technischen Universität München zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr. Massimo Fornasier

Prüfer der Dissertation:

1. Univ.-Prof. Dr. Michael M. Wolf
2. Univ.-Prof. Dr. Dr. Holger Boche
3. Univ.-Prof. Dr. David Gross (nur schriftliche Beurteilung),
   Universität Köln

Die Dissertation wurde am 05.09.2016 bei der Technischen Universität München eingereicht und durch die Fakultät für Mathematik am 06.10.2016 angenommen.

Acknowledgements

First, I want to thank Prof. Michael Wolf for supervising my doctorate. Initially, he provided me with interesting questions to work on and subsequently gave me more and more room to develop and also realize own research ideas, thereby creating a productive and enjoyable working environment.

I also want to thank Prof. Holger Boche for the support and advice he provided in the cause of my doctoral studies.

I am very grateful to my collaborators Claudio Carmeli, Teiko Heinosaari, Felix Krahmer, Jussi Schulz, Alessandro Toigo and Péter Vrana. I enjoyed working with you.

For their time and effort I would like to thank the committee members Prof. David Gross, Prof. Holger Boche and Prof. Massimo Fornasier.

For proof-reading the introductory part of this dissertation I am very grateful to Prof. Robert König, Prof. Michael Keyl and Dr. Teiko Heinosaari.

Furthermore, I would like to thank all the members of M5 for the great atmosphere and cohesion in our group.

Finally, I am deeply grateful to my parents, Gerhard and Beatrix Kech, as well as my girlfriend, Marina Ineichen, for the support they provided.

List of contributed articles

I) M. Kech, P. Vrana and M.M. Wolf,
The Role of Topology in Quantum Tomography,
Journal of Physics A: Mathematical and Theoretical, vol. 48, no. 26, June 2015

II) M. Kech and M.M. Wolf,
Constrained Quantum Tomography of Semi-Algebraic Sets with Applications to Low-Rank Matrix Recovery,
arXiv:1507.00903, recommended for publication in Information and Inference: a Journal of the IMA, July 2016

III) M. Kech,
Explicit Frames for Deterministic Phase Retrieval via PhaseLift,
arXiv:1508.00522, recommended for publication in Applied and Computational Harmonic Analysis, July 2016

IV) M. Kech and F. Krahmer,
Optimal Injectivity Conditions for Bilinear Inverse Problems with Applications to Identifiability of Deconvolution Problems,
arXiv:1603.07316, submitted to SIAM Journal on Applied Algebra and Geometry, March 2016

V) C. Carmeli, T. Heinosaari, M. Kech, A. Toigo and J. Schultz,
Stable Pure State Quantum Tomography from Five Orthonormal Bases,
arXiv:1604.02970, to appear in Europhysics Letters, August 2016

VI) M. Kech,
Dynamical Quantum Tomography,
arXiv:1605.06786, submitted to Journal of Mathematical Physics, January 2016

The author of the present dissertation was the principal author of all the articles listed above.

Contents

1

Introduction

Inferring properties of a physical system from measurement data is a cornerstone of physical science. By inferring sufficiently many properties one can completely characterize a system in the following sense: Physical models approximately describe certain traits of a system by a set of parameters from which all model-specific predictions can be computed. Consequently, within the context of this model, inferring these parameters from measurement data gives a complete description of the system. For instance, when modelling air as an ideal gas it can be completely characterized by measuring pressure, volume and temperature.

The present dissertation is concerned with inferring such complete descriptions or initial conditions in the context of quantum mechanics. Quantum mechanics is an intrinsically probabilistic theory: Even when knowing the initial conditions of a quantum system, in general the outcome of a measurement cannot be predicted. Only the probability with which an outcome occurs in a statistical experiment can be determined. A full description of a quantum system is provided by its state, which is a complete specification of the outcome distributions of all possible measurements. One can take the viewpoint that a state provides a description of a statistical ensemble of quantum systems rather than that of an individual system. Form this perspective quantum state tomography is the process of inferring the unknown state of an ensemble of quantum systems from the data obtained by performing measurements on instances of the ensemble. It is a vital routine in quantum information science where it is used to test processing devices. However, with growing system size quantum tomography quickly becomes a challenging task and sometimes infeasible. For instance, to determine a maximum likelihood estimate of a quantum state of eight ions required hundreds of thousands of measurements and weeks of post-processing in an experiment conducted by Häffner et al. [1]. However, as the

experimenter typically has some prior information about the state he wants to identify, only the subset of states consistent with this information has to be considered for tomography. For example, it could be known that the state is pure, has certain symmetries or is a ground state of a local Hamiltonian. In such cases one can hope for a more efficient tomography and indeed, based on ideas of compressed sensing, a practical protocol for the tomography of low-rank quantum states was provided in [2, 3].

Following similar lines of research, the present dissertation is concerned with how and to what extent prior information about a quantum system can be utilized for a more efficient tomography procedure. The prior information is typically given in terms of a predefined subset of the state space together with the promise that the quantum state to be measured is contained in or at least close to this subset. Given such a subset, the focus is on the following three issues:

1. What is the minimal number of measurement outcomes necessary to discriminate any two quantum states of the subset?

2. Can this minimal number of measurement outcomes be reached when restricting to a class of admissable measurement settings as for instance projective measurements?

3. Can one find measurement settings with a close to minimal number of outcomes, which allow for a stable and computationally tractable reconstruction of every quantum state of the subset?

The first two issues are addressed for rather general subsets. For the last issue the analysis focuses on quantum states of bounded rank. Similar questions are analyzed in the context of other signal processing tasks such as phase retrieval or deconvolution problems.

The focus of the present dissertation is mainly on the number of measurement outcomes. The question of how many identically prepared quantum systems are needed to estimate an unknown quantum state to a given precision level is not regarded[1].

In the remainder of this introduction, a brief summary of the six articles included in the present dissertation is given. The main results as well as the methods used to obtain them are discussed and connections to existing literature are pointed out.

In the second chapter, mathematical and technical foundations are presented. First, the basic notions of finite-dimensional quantum mechanics are introduced, followed by a brief introduction to quantum state tomography. Finally, the last part of this chapter is concerned with

[1] In the context of phase retrieval and blind deconvolution this issue need not be considered as the sampling problem does not arise.

quantum state tomography in the scenario where prior information constrains the set of relevant states to a subset of lower dimensionality. The focus is on results and concepts from the existing literature which are particularly relevant for the present dissertation.
These two chapters are followed by the contributed articles ordered according to their publication date. Each article is preceded by a short technical summary of its main results.

1.1 Summary and Discussion of Results

The articles included in the present dissertation can be classified with respect to the issues 1, 2 and 3, yet, here they are ordered according to their publication date. As the tomography of bounded rank quantum states is closely related to topics in signal processing such as phase retrieval, low-rank matrix recovery or deconvolution, some of the articles are targeted towards these lines of research (articles III, IV).

1. *Article I: The Role of Topology in Quantum Tomography*

   This article is concerned with Issue 1 in scenarios where prior information effectively restricts the state space to a smooth manifold of lower dimensionality. More precisely, it approaches the following question: Given a smooth manifold embedded in the state space, what is the minimal number of binary measurement settings[1] required to discriminate any two distinct states of the manifold? It is assumed that every setting can be measured arbitrarily often, resulting in a precise knowledge of all the binary outcome distributions.

   The basic idea is that the minimal number of binary measurement settings is essentially determined by topological obstructions. For instance, if the manifold is homeomorphic to a Klein bottle one would expect that at least four measurement settings are needed as the Klein bottle cannot be continuously mapped into three-dimensional Euclidean space without self-intersections. In the context of quantum tomography, topological arguments were first deployed in [4] to determine, i.a., the minimal number of binary measurement settings necessary to discriminate any two pure quantum states up to logarithmic corrections. The respective analysis is based on results concerning embeddings of complex projective space into Euclidean space [5, 6]. However, as the argument given in [4] relies on a specific technical assumption, it remained unclear for which manifolds the topological reasoning is valid.

[1] Equivalently, one can ask for the minimal number of outcomes of a generalized measurement.

This article introduces a general framework showing that under mild stability assumptions on the measurements, the topological reasoning is valid for arbitrary smooth manifolds. More precisely, considering a measurement procedure as a smooth mapping from the manifold to Euclidean space, the argument solely relies on the assumption that this map is a smooth embedding. It is then shown that the embedding property is equivalent to two mild stability properties a practical measurement procedure should satisfy. In addition, when allowing for measurements on several copies of the state, it is shown that the minimal number of binary measurement settings needed to discriminate any two states of a given manifold is precisely the minimal dimension of Euclidean space the manifold can be embedded into. The approach is then applied to states with bounded rank, taken from a unitary orbit and invariant under a given unitary symmetry. The topological reasoning only yields lower bounds on the minimal number of binary measurement settings. By means of explicit constructions, also upper bounds are provided. In most cases the upper and lower bounds are reasonably close, demonstrating the success of the topological approach in these scenarios.

It remains an open problem to what extent the lower bounds obtained in this article apply to practical measurement devices as relevant aspects such as the complexity of the necessary post-processing of the measurement data or the ability to verify the assumed prior information are not considered in the analysis. However, the results of the articles III and V suggest that they can be reasonably tight also in more realistic scenarios.

2. *Article II: Constrained Quantum Tomography of Semi-Algebraic Sets with Applications to Low-Rank Matrix Recovery*

   This article is concerned with Issue 2. In practice, an experimenter typically cannot implement an arbitrary (generalized) measurement, but only has access to a limited class of realizable measurements. For instance, this class could be the set of von Neumann measurements or, when dealing with mutipartite systems, the set of local measurements. This raises the following question: Given a subset of the state space, are there natural classes of measurements for which an efficient tomography procedure is possible? Article II approaches this problem with regards to the minimal number of measurement outcomes leading to the related question: Given a set of states and a class of admissible measurements, is there an admissible measurement whose number of outcomes is comparable to the topological lower bound that can discriminate any two states of the set? Phrased

differently, this article is concerned with finding upper bounds on the minimal number of measurement outcomes necessary to discriminate any two distinct states of a given subset of the state space in scenarios where the class of admissible measurements is restricted.

The case of pure state tomography with von Neumann measurements was considered in [7, 8, 9], where it is shown that any two pure states can be discriminated by merely four von Neumann measurements. For dimensions greater than four this result is known to be sharp [9]. In the context of phase retrieval and low-rank matrix recovery, similar results were obtained in [10, 11, 12, 13, 14, 15].

Motivated by the algebraic geometry approach taken in [10], Article II extends these results by showing that von Neumann measurements, or more generally rank one measurements, are in a certain sense suited for state discrimination on arbitrary semi-algebraic subsets of the state space. From this, a Whitney type embedding result can be proven straightforwardly: There is a collection of von Neumann measurements which can discriminate any two distinct elements of a given set of states as long as their cumulative number of independent outcomes exceeds twice the set's dimension. Considering specific subsets, it is shown that any two quantum states of rank at most r can be discriminated by essentially the minimal number of von Neumann measurements. In addition, similar results are provided for measuring expectation values of local observables.

The algebraic arguments used in this article allow for a rather general analysis of the state discrimination problem. However, these techniques have the drawback that some aspects which are essential for a practical tomography procedure cannot be regarded. For instance, error tolerance is crucial because of imperfect prior information and the statistical nature of quantum state tomography. However, although a qualitative stability analysis is possible, the algebraic techniques cannot provide quantitative stability guarantees. Another drawback of the algebraic approach is that it does not yield efficient recovery algorithms.

Rather than providing practical measurement devices, the purpose of this article is to identify interesting measurement schemes, like, e.g., von Neumann measurements, that allow tomography on subsets of the state space. Furthermore, the techniques can be combined with those of Article I to establish fundamental bounds on the minimal number of measurement settings needed for state discrimination, as is done in case of discriminating

low-rank quantum states with von Neumann measurements. These bounds can then serve as a benchmark for practical measurement devices.

3. *Article III: Explicit Frames for Deterministic Phase Retrieval via PhaseLift*
   This article addresses Issue 3 in the context of phase retrieval, which is the task of reconstructing a signal up to a global phase from intensity measurements. Phase retrieval is mathematically closely related to the tomography of pure quantum states. One of the most prominent applications of phase retrieval arguably is X-ray crystallography, which aims to reconstruct the electron density of a crystal from X-ray diffraction patterns.

   Based on ideas from matrix recovery [16, 17], the PhaseLift approach [18, 19, 20] provides a stable and computationally tractable recovery scheme for phase retrieval: First, by a lifting step, the recovery problem is formulated as a linearly constrained rank minimization problem and in a second step relaxed to a convex program. It is then shown that an n-dimensional signal can be recovered up to a global phase by means of PhaseLift in the sense that the convex relaxation is precise with high probability if $\mathcal{O}(n)$ randomly chosen intensity measurements are performed. Furthermore, the recovery is also stable with respect to noise.

   Article III pursues a deterministic approach to PhaseLift. Motivated by the results given in [21], for any dimension n, the article provides $5n-6$ intensity measurements such that every signal can be recovered up to a global phase by solving the relaxed optimization problem. Indeed, this is the smallest known number of intensity measurements for which a computationally tractable recovery is possible and the first explicit construction of a small collection of measurements which allow uniform recovery via PhaseLift. These results are also generalized to the recovery of low-rank positive matrices. The employed recovery procedure is stable with respect to noise in the sense that the reconstruction error scales linearly in the noise level. However, as the constant of proportionality is not estimated, this result does not imply stability in a practical sense.

   While the convex programs used in the PhaseLift approach are in principle computationally tractable, solving them becomes impractical for large signal dimensions. Concerning the cost of computation, there are more favourable approaches as for instance those proposed in [22, 23]. Based on $6n-3$ intensity measurements, another deterministic approach to phase retrieval which makes use of a different recovery scheme was introduced in [24, 25].

4. *Article IV: Optimal Injectivity Conditions for Bilinear Inverse Problems with Applications to Identifiability of Deconvolution Problems*

   This article is concerned with issues 1 and 2 in the context of bilinear inverse problems, i.e., inverse problems where the task is to recover two inputs, the signal and the filter, from bilinear measurements. Practically relevant instances of such inverse problems are for instance blind deconvolution[1] [26, 27, 28, 29, 30] or self-calibration problems [31, 32]. Again by a lifting approach, a bilinear inverse problem can be formulated as a linearly constrained rank minimization problem. However, one often has to make additional structural assumptions on the input pair since many problems, such as blind deconvolution, are otherwise ill-posed.

   Identifiability for bilinear inverse problems under sparsity constraints is the question whether a sparse input pair is unambiguously determined by the measurement outcomes. It was first considered in [33, 34], in particular providing negative results for the case of blind deconvolution. In [35] these cases were identified as exceptional in the sense that the dictionary pairs for which given inputs are not identifiable have measure zero if the inputs' sparsity level is low enough. Near optimal identifiability results were provided in [36], where the analysis was furthermore extended to injectivity, i.e., uniform identifiability over all sparse enough input pairs.

   Different from [33, 34, 35, 36], Article IV is based on techniques from algebraic geometry. These techniques are used to improve the results given in [36] and also to show the optimality of the resulting conditions. More precisely, the article provides a lower bound on the number of outcomes of a bilinear map capable of discriminating any two input pairs of given sparsity level. As this result holds for arbitrary bilinear maps and dictionaries, in particular it yields an upper bound on the input sparsity level up to which blind deconvolution is possible. This bound is tight, as it is shown to be attained by generic dictionary pairs.

   The argument which yields the dictionary pairs attaining the lower bound is based on the approach taken in Article II. Consequently, the results do not entail tractable reconstruction algorithms. However, the optimal identifiability bounds obtained in this article can be used as a benchmark for future research on bilinear inverse problems.

[1] Blind deconvolution is the specific bilinear inverse problem where the bilinear map is the circular convolution.

5. *Article V: Stable Pure State Quantum Tomography from Five Orthonormal Bases*
   This article addresses Issue 3 in the context of pure state tomography which, as mentioned before, is closely related to phase retrieval.

   Motivated by ideas from compressed sensing, in [2, 3] tomography procedures are proposed which allow the stable and computationally tractable recovery of low-rank quantum states from few measurement outcomes. In particular, it is shown that an arbitrary pure state of a d-qubit system can be efficiently reconstructed with high probability from $\mathcal{O}(n \ln n)$ Pauli measurements drawn at random, where $n := 2^d$. Using different proof techniques, improved stability results are provided in [37, 38]. Furthermore, in [38] an analysis of the sample complexity is given. From a practical point of view however, it may be favourable to implement an explicitly specified measurement setup rather than a random one. Such a deterministic recovery scheme based on five von Neumann measurements was proposed and experimentally demonstrated in [39]. However, as their scheme is adaptive, i.e., the outcome distribution of the first measurement affects the choice of the subsequent ones, the actual number of needed von Neumann measurements is significantly higher if the procedure is required to work uniformly for all pure states.

   Article V provides a recovery scheme which is both deterministic and non-adaptive, thereby overcoming the mentioned drawbacks of [2, 3, 39]: For any dimension, five von Neumann measurements are constructed which allow the recovery of every pure state by means of a convex program. Conceptually, the taken approach is similar to the one of Article III, however the argument is considerably simplified (yet less general) by following a different proof strategy. As compared to Article III, the main technical advance is to realize the additional structure von Neumann measurements entail. This is achieved by generalizing a construction given in [8]. As the stability results provided in Article III transfer directly, the recovery is also stable, but again quantitative stability guarantees are not available. Therefore, numerical simulations are performed which indicate a reasonable noise tolerance in practice.

6. *Article VI: Dynamical Quantum Tomography*
   This article is concerned with Issue 2. Originating from the approach presented in Article II, quantum tomography is considered in the following scenario: The experimenter is given a fixed measurement setup and has to identify the state of an ensemble of quantum systems. Before measuring with the setup on a system of the ensemble, he can subject

the system to a known time evolution for a desired period of time. For a suitable time evolution, a setup with just few outcomes renders an informationally complete state tomography possible. For instance, given an ensemble of identically prepared electrons, by performing a Stern-Gerlach experiment only one component of the spin can de determined. However, if the electrons are subjected to a suitably directed magnetic field for different time periods before performing the measurement, the spin can be completely recovered.

In this article, it is shown that for suitable unitary time evolutions any state of a d-level system can be uniquely identified by measuring with a setup which has d outcomes at $d+1$ equidistant time points. This result is tight in the sense that the previous statement cannot hold for a setup with fewer outcomes also if measuring at more time points. Furthermore, when considering more general time evolutions, it is shown that a binary setup suffices. Vaguely speaking, this shows that any state can be completely identified by the time evolution of a single observable's expectation value[1]. It is shown that the measurement scheme also is well-suited for state discrimination on subsets of the state space, where good upper bounds on the number of required time points are provided.

As the approach taken in this article is based on the one taken in Article II, it has similar drawbacks (see summary of Article II).

[1] This only holds when both the observable and the time evolution are chosen suitably.

2

Methods

In this chapter, a brief introduction to basic mathematical and physical concepts of quantum mechanics is provided and some results on quantum state tomography are summarized. As the articles included in the present dissertation are exclusively concerned with finite-dimensional quantum mechanics, the exposition is restricted to this case, thereby avoiding technical subtleties the infinite-dimensional theory entails. Throughout this chapter, references for basic definitions and some basic results from quantum information theory and differential topology are omitted. Concerning quantum information theory, the reader may for instance consult the book by Michael A. Nielsen and Isaac L. Chuang [40]. Definitions and results related to differential topology can be found in the books [41, 42]. The author does not claim ownership for the results presented in this chapter, even if a reference is omitted.

In Section 2.1, a brief introduction to quantum mechanics is provided, where both the physical concepts as well as their mathematical description are considered. Due to their relevance in the following, measurements are discussed in somewhat more detail. Quantum states and measurements are introduced in Section 2.1.1 and Section 2.1.2 is concerned with time evolutions in quantum mechanics.

In Section 2.2, an introduction to quantum state tomography is provided. The estimation problem involved in reconstructing a quantum state from measurement data is explained. Furthermore, some estimation techniques are briefly discussed.

Section 2.3 is concerned with quantum state tomography in the scenario where prior information restricts the set of relevant states to a subset of lower dimensionality. In this section, the focus is mainly on Issue 1, i.e., on the number of measurement outcomes necessary to discriminate any two states of the subset. Essentially this section summarizes results and ideas

given in [4]. First, measurements are analyzed from a topological point of view and afterwards as smooth mappings from the state space to Euclidean space. The gained insight is then used to lower bound the number of binary measurement settings required to discriminate any two pure states. This approach serves as a starting point for the analysis given in Article I. Additionally, a result showing that the obtained lower bound is close to optimal is presented. The given proof motivates the approach taken in the articles II and VI.

Finally, in Section 2.4, the compressed sensing approach to quantum state tomography is presented (see [2, 3, 37, 38]), which addresses Issue 3 for quantum states of rank at most r. Article V is closely related to these articles as it aims at similar results and utilizes similar convex programs for the recovery. From a technical point of view however, the approach taken in Article V is very different from the probabilistic approaches taken in [2, 3, 37, 38]. The discussion focuses on [37, 38], where an analysis based on the restricted isometry property (see [16]) is given.

Notation

Throughout this chapter, $(\mathcal{H}, \langle\cdot,\cdot\rangle)$ denotes a Hilbert space of finite dimension n and $\|\cdot\| = \sqrt{\langle\cdot,\cdot\rangle}$ denotes the associated norm. In the following, the explicit specification of the scalar product often is omitted. The set of linear operators $B : \mathcal{H} \to \mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$. Given Hilbert spaces $(\mathcal{H}_1, \langle\cdot,\cdot\rangle_1)$, $(\mathcal{H}_2, \langle\cdot,\cdot\rangle_2)$, the adjoint of an operator $B : \mathcal{H}_1 \to \mathcal{H}_2$ is the unique operator $B^* : \mathcal{H}_2 \to \mathcal{H}_1$ such that $\langle x, B^*y\rangle_1 = \langle Bx, y\rangle_2$ holds for all $x \in \mathcal{H}_1$, $y \in \mathcal{H}_2$. Furthermore, $H(\mathcal{H}) := \{B \in \mathcal{L}(\mathcal{H}) |\, B^* = B\}$ denotes the set of self-adjoint operators. An operator $B \in \mathcal{L}(\mathcal{H})$ is called positive, written as $B \geq 0$, if and only if (iff) B is self-adjoint with non-negative eingenvalues. In the following, $\mathcal{L}(\mathcal{H})$ is viewed as a Hilbert space equipped with the Hilbert-Schmidt inner product, $\langle A, B\rangle_{HS} := \mathrm{tr}(A^*B)$, $\forall A, B \in \mathcal{L}(\mathcal{H})$. The Hilbert-Schmidt norm is denoted by $\|\cdot\|_{HS}$. The set of all unitary operators on $\mathcal{H}$ is denoted by $U(\mathcal{H})$. The complex span of a set of operators $\mathcal{B} \subseteq \mathcal{L}(\mathcal{H})$ is denoted by $\mathrm{Span}\,\mathcal{B}$.

By choosing an orthonormal basis, $\mathcal{H}$ is sometimes identified with $\mathbb{C}^n$ equipped with the standard inner product. Under this identification an operator $B \in \mathcal{L}(\mathcal{H})$ has a concrete representation as a complex $n \times n$ matrix. The Euclidean norm on both $\mathbb{C}^n$ and $\mathbb{R}^n$ is denoted by $\|\cdot\|$. The transpose and conjugate transpose of an $n \times m$ matrix $A \in \mathbb{C}^{n\times m}$ is denoted by A^t and A^*, respectively.

2.1 Finite-dimensional Quantum Mechanics

2.1.1 Quantum States and Measurements

Conceptually, it is useful to split an experiment into two steps, preparation and measurement[1]. Specifying the preparation procedure of a quantum system determines the outcome probabilities of all possible measurements. From this perspective, a quantum state can be understood as the equivalence class of preparation procedures yielding identical outcome probabilities for all measurements. Similarly, a measurement can be understood as the equivalence class of measurement procedures which yield identical outcome distributions (in a statistical experiment) for all quantum states. The following correspondence rules connect these physical concepts to the mathematical objects introduced before.

Rule 1. (Quantum state). A quantum state corresponds to a positive linear operator ϱ on $\mathcal{H}$ with normalization $\mathrm{tr}(\varrho) = 1$, i.e., to an element of $\mathcal{S}(\mathcal{H}) := \{\varrho \in \mathcal{L}(\mathcal{H}) |\, \varrho \geq 0,\ \mathrm{tr}(\varrho) = 1\}$. The set $\mathcal{S}(\mathcal{H})$ is called state space.

In the following, the term quantum state is used for both the physical concept, its mathematical description as an element of $\mathcal{S}(\mathcal{H})$ and its concrete matrix representation when identifying $\mathcal{H}$ with $\mathbb{C}^n$. The set of quantum states is compact as well as convex and the set of its extreme points, called pure states, is given by[2]

$$\mathcal{S}_1(\mathcal{H}) := \{\rho \in \mathcal{S}(\mathcal{H}) |\, \rho^2 = \rho\} = \{\psi\psi^* |\, \psi \in \mathcal{H},\ \|\psi\| = 1\}.$$

The set of quantum states of rank at most r is denoted by

$$\mathcal{S}_r(\mathcal{H}) := \{\varrho \in \mathcal{S}(\mathcal{H}) |\, \mathrm{rank}\, \varrho \leq r\}.$$

Rule 2. (POVM). A measurement corresponds to a positive operator valued measure (POVM) on $\mathcal{H}$, i.e., to a mapping $P : 2^I \to \mathcal{L}(\mathcal{H}),\ A \mapsto \sum_{i \in A} P_i$, where I is a finite set labelling all possible measurement outcomes and $\{P_i\}_{i \in I}$ is an indexed family of positive operators such that $P(I) = \sum_{i \in I} P_i = \mathbb{1}_{\mathcal{H}}$.

The elements of $\{P(\{i\})\}_{i \in I}$, $P \in POVM_{\mathcal{H}}$, are called effect operators. The set of all POVMs on $\mathcal{H}$ is denoted by $POVM_{\mathcal{H}}$. The normalization and positivity conditions for both quantum states and POVMs ensure that for all $\varrho \in \mathcal{S}(\mathcal{H})$, the map $2^I \ni A \mapsto \langle P(A), \varrho \rangle_{HS} \in [0, 1]$ is a

[1] The ambiguity of this step is not problematic as different splits lead to equivalent descriptions.
[2] $\psi\psi^*$ is the element of $H(\mathcal{H})$ which acts on any $\xi \in \mathcal{H}$ as $(\psi\psi^*)(\xi) := \psi\langle\psi, \xi\rangle$.

probability measure over $(I, 2^I)$. Therefore, a POVM P represents a measurement in the sense that it associates to a quantum state ρ the probability measure

$$p_{P,\varrho} := \langle P, \varrho \rangle_{HS}$$

over the set of measurement outcomes. If not stated otherwise, in the following it is assumed that for each POVM $P : 2^I \to \mathcal{L}(\mathcal{H})$ with m outcomes one has $I = \{1, 2, \ldots, m\}$. In order to simplify the presentation, the one-to-one correspondence between POVMs $P \in POVM_{\mathcal{H}}$ and their associated indexed families of effect operators $\{P(\{i\})\}_{i \in I}$ is sometimes exploited by writing $P = \{P(\{i\})\}_{i \in I}$.

A different yet closely related way to describe measurements is in terms of observables. An observable O is a self-adjoint element of $\mathcal{L}(\mathcal{H})$. Let $\{\lambda_1, \ldots, \lambda_m\}$ be the set of eigenvalues of the observable O and $\{P_1, \ldots, P_m\}$ be the set of associated spectral projections. As $\{P_1, \ldots, P_m\}$ is a set of positive operators with $\sum_{i=1}^m P_i = \mathbb{1}_{\mathcal{H}}$, the map $P : 2^{\{1,\ldots,m\}} \ni A \mapsto \sum_{i \in A} P_i \in \mathcal{L}(\mathcal{H})$ is a POVM. The observable O is then understood as the equivalence class of measurement procedures characterized by P and furthermore each eigenvalue λ_i is understood as the measurement result corresponding to the event $i \in \{1, \ldots, m\}$. With this interpretation, $\langle O, \varrho \rangle_{HS} = \sum_{i=1}^m \lambda_i \langle P_i, \varrho \rangle_{HS} = \sum_{i=1}^m \lambda_i p_{P,\varrho}(\{i\})$ is the expectation value of O for an ensemble of quantum systems prepared in state $\varrho \in \mathcal{S}(\mathcal{H})$. The POVMs which are induced by observables are called projective measurements. If in addition all effect operators are rank one, a projective measurement is called von Neumann measurement. Clearly, projective measurements are more restrictive than POVMs which are sometimes called generalized measurements for this reason. However, the two notions are closely related in the sense that each POVM can be lifted to a projective measurement on a larger system.

Theorem 1 (Naimark's dilation theorem)**.** *Let $P \in POVM_{\mathcal{H}}$ be a POVM. Then, there exists a Hilbert space $\mathcal{H}'$, a linear isometry $V : \mathcal{H} \to \mathcal{H}'$ and a projective measurement $P' \in POVM_{\mathcal{H}'}$ with the same number of outcomes as P such that for all $\varrho \in \mathcal{S}(\mathcal{H})$ one has*

$$\langle P, \varrho \rangle_{HS} = \langle P', V \varrho V^* \rangle_{HS}.$$

Proof. The proof given here closely follows the proof of Theorem 2.6 in [43]. Let $e_1, \ldots, e_n$ be an orthonormal basis (ONB) of $\mathcal{H}$ and let $P \in POVM_{\mathcal{H}}$ be such that for all $i \in I = \{1, \ldots, m\}$ there exists $\psi_i \in \mathcal{H}$ with $P(\{i\}) = \psi_i \psi_i^*$. Let $\mathcal{H}'$ be an m-dimensional Hilbert space and let $f_1, \ldots, f_m$ be an ONB of $\mathcal{H}'$. Define the linear map $V : \mathcal{H} \to \mathcal{H}'$ by setting $V e_i = f_i$ for all $i \in \{1, \ldots, n\}$. Since $\sum_{i=1}^m \psi_i \psi_i^* = \mathbb{1}_{\mathcal{H}}$, the $n \times m$ matrix $M_{ij} := \langle e_i, \psi_j \rangle$ is an isometry. Therefore, M can be extended to an $m \times m$ unitary matrix $\tilde{M}$. Then, the vectors $\tilde{\psi}_j := \sum_{i=1}^m \tilde{M}_{ij} f_i,\ j \in \{1, \ldots, m\}$, form an orthonormal basis. Define a POVM $P' \in POVM_{\mathcal{H}}$

by setting $P'(\{j\}) := \tilde{\psi}_j \tilde{\psi}_j^*$ for all $j \in \{1, \dots, m\}$. Then, it follows by construction that $\langle P(\{j\}), \varrho \rangle_{HS} = \langle P'(\{j\}), V \varrho V^* \rangle_{HS}$ holds for all $\varrho \in \mathcal{S}(\mathcal{H})$ and $j \in \{1, \dots, m\}$.

Now consider the case where the rank of the operators $P(\{i\})$, $i \in I$, is arbitrary. For every $i \in I$ let $P(\{i\}) = \sum_{j=1}^{\alpha_i} P_{i,j}$ be a spectral decomposition into rank one elements and define a POVM $\tilde{P} \in POVM_{\mathcal{H}}$ with $\sum_{i=1}^{m} \alpha_i$ outcomes by setting $\tilde{P}(\{(i,j)\}) = P_{i,j}$ for each $(i,j) \in \tilde{I} := \{(i,j)\}_{i \in I, j \in \{1,\dots,\alpha_i\}}$. Proceeding as in the case of rank one effect operators, one obtains a Hilbert space $\mathcal{H}'$, a linear isometry V and a POVM $\tilde{P}' \in POVM_{\mathcal{H}'}$. Finally, setting $P'(\{i\}) := \sum_{j=1}^{\alpha_i} \tilde{P}'(\{(i,j)\})$ for all $i \in I$ yields a POVM $P' : 2^I \to \mathcal{L}(\mathcal{H})$ with the desired properties. □

Remark 2. *Let $P \in POVM_{\mathcal{H}}$ be a POVM such that every element of $\{P(\{i\})\}_{i \in I}$ is rank one. Then, the above construction shows that one can choose $\mathcal{H}'$ with $\dim \mathcal{H}' = m$. Furthermore, the construction yields a von Neumann measurement in this case.*

Composite quantum systems are described by means of tensor products. More precisely, when considering $k \in \mathbb{N}$ distinct quantum systems with state spaces $\mathcal{S}(\mathcal{H}_1), \dots, \mathcal{S}(\mathcal{H}_k)$ and sets of POVMs $POVM_{\mathcal{H}_1}, \dots, POVM_{\mathcal{H}_k}$ the state space and the set of POVMs of the composite system are given by $\mathcal{S}(\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_k)$ and $POVM_{\mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_k}$, respectively. Given a quantum state $\varrho \in \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ on a composite system the reduced state of the first system is given by $\mathrm{tr}_2(\varrho) := (\mathbb{1}_{\mathcal{L}(\mathcal{H}_1)} \otimes \mathrm{tr})(\varrho)$, where $\mathrm{tr} : \mathcal{H}_2 \mapsto \mathbb{C}$ is the trace associated to the second system.

From Theorem 1 it can be shown in a straightforward way that any POVM can be implemented as a projective measurement on a composite system.

Corollary 3. *Let $P \in POVM_{\mathcal{H}}$ be a POVM. Then, there exists a Hilbert space $\mathcal{H}_E$, a projective measurement $P' \in POVM_{\mathcal{H} \otimes \mathcal{H}_E}$ with the same number of outcomes as P and a pure state $\sigma \in \mathcal{S}_1(\mathcal{H}_E)$ such that for all $\varrho \in \mathcal{S}(\mathcal{H})$ one has*

$$\langle P, \varrho \rangle_{HS} = \langle P', \varrho \otimes \sigma \rangle_{HS}.$$

Proof. Let $e_1, \dots, e_n$ be an ONB of $\mathcal{H}$ and let $P \in POVM_{\mathcal{H}}$ be such that for all $i \in I = \{1, \dots, m\}$ there exists $\psi_i \in \mathcal{H}$ with[1] $P(\{i\}) = \psi_i \psi_i^*$. Let $\mathcal{H}_E$ be an n_E-dimensional Hilbert space such that $n \cdot n_E \geq m$ and let $f_1, \dots, f_{n_E}$ be an ONB of $\mathcal{H}_E$. Define a linear isometry $V : \mathcal{H} \mapsto \mathcal{H} \otimes \mathcal{H}_E$ by setting $V(e_i) = e_i \otimes f_1$ for all $i \in \{1, \dots, n\}$ and let $\sigma = f_1 f_1^*$. Let $\mathcal{H}' \subseteq \mathcal{H} \otimes \mathcal{H}_E$ be an m-dimensional subspace of $\mathcal{H} \otimes \mathcal{H}_E$ containing $V(\mathcal{H})$ and let $\mathcal{H}' \oplus \mathcal{H}'_\perp \simeq \mathcal{H} \otimes \mathcal{H}_E$ be the associated orthogonal decomposition. With this choice of V and $\mathcal{H}'$ one can proceed as in the proof of Theorem 1 to obtain a projective measurement $\tilde{P}' \in POVM_{\mathcal{H}'}$. To conclude the proof, define the projective measurement $P' \in POVM_{\mathcal{H} \otimes \mathcal{H}_E}$ by setting $P'(\{i\}) = \tilde{P}'(\{i\}) \oplus 0$ for $1 \leq i < m$ and $P'(\{m\}) = \tilde{P}'(\{m\}) \oplus \mathbb{1}_{\mathcal{H}'_\perp}$. □

[1] For higher rank operators $\{P(\{i\})\}_{i \in I}$ consult the respective part in the proof of Theorem 1.

2.1.2 Time Evolution in Quantum Mechanics

Taking the viewpoint that time evolutions act on quantum states rather than measurement procedures leads to the following correspondence rule.

Rule 3. (Time evolution). A time evolution corresponds to a map $\mathcal{S}(\mathcal{H}) \ni \varrho \mapsto \mathcal{T}(\varrho) \in \mathcal{S}(\mathcal{H})$, where $\mathcal{T} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is linear, trace-preserving, i.e., $\mathrm{tr}(\mathcal{T}(X)) = \mathrm{tr}(X)$ for all $X \in \mathcal{L}(\mathcal{H})$, and completely positive[1], i.e., $(\mathbb{1}_{\mathcal{H}'} \otimes \mathcal{T})(X) \geq 0$ for all finite-dimensional Hilbert spaces $\mathcal{H}'$ and all $X \in \mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$ with $X \geq 0$.

The set of all linear maps $\mathcal{T} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ which are completely positive and trace-preserving (CPTP) is denoted by $CPTP_{\mathcal{H}}$. CPTP maps allow the following representation.

Theorem 4 (Kraus representation, [44, 45]). *A linear map $\mathcal{T} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is completely positive iff there is a number $k \in \mathbb{N}$ and operators $A_i \in \mathcal{L}(\mathcal{H}),\ i = 1, \ldots, k$, such that for any $X \in \mathcal{L}(\mathcal{H})$ one has*

$$\mathcal{T}(X) = \sum_{i=1}^{k} A_i X A_i^*.$$

The operators $A_i,\ i = 1, \ldots, k$, are called Kraus operators of $\mathcal{T}$ and $\mathcal{T}$ is trace-preserving iff $\sum_{i=1}^{k} A_i^* A_i = \mathbb{1}_{\mathcal{H}}$.

Closed quantum systems, i.e., quantum systems with a physically reversible time evolution, are often considered separately. Physically reversible time evolutions correspond to the subset $\{\mathcal{T} \in CPTP_{\mathcal{H}} | \, \exists U \in U(\mathcal{H}) : \mathcal{T}(B) = UBU^*, \forall B \in \mathcal{L}(\mathcal{H})\}$ of CPTP maps. Similar to the case of POVMs and von Neumann measurements, every CPTP map can be realized as the restriction of reversible dynamics on a composite system to a subsystem.

Theorem 5 (Stinespring dilation, [46]). *A linear map $\mathcal{T} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is CPTP iff there exists a finite-dimensional Hilbert space $\mathcal{H}'$, a unitary operator $U \in U(\mathcal{H} \otimes \mathcal{H}')$ and a quantum state $\sigma \in \mathcal{S}_1(\mathcal{H})$ such that for all $X \in \mathcal{L}(\mathcal{H})$ one has*

$$\mathcal{T}(X) = tr_2(U(X \otimes \sigma)U^*).$$

2.2 Quantum State Tomography

Quantum state tomography aims to identify a preparation procedure, or more precisely the quantum state $\varrho \in \mathcal{S}(\mathcal{H})$ it corresponds to. The preparation procedure can be viewed as a black

[1] This requirement ensures that quantum states are mapped to quantum states also if the time evolution is only applied to a subsystem of a composite system.

box which, on invocation, outputs a quantum system prepared accordingly. In order to identify the quantum state ϱ of the black box, experiments of the following kind can be repeatedly performed: One invokes the black box to obtain a quantum system and then performs a measurement procedure. Note that the experimenter could use different measurement procedures in different experiments. Performing such an experiment with a procedure characterized by a POVM $P : 2^I \to \mathcal{L}(\mathcal{H})$ yields an outcome which is understood as an (independent) realization of a random variable R with values in I distributed according to the probability vector $p := (\langle P(\{i\}), \varrho\rangle_{HS})_{i=1}^m \in \mathbb{R}^m$. Hence, repeating the experiment with P fixed yields independent realizations of R and consequently the observed relative frequencies give an empirical estimate of p. The goal is then to infer ϱ from the measurement data, i.e., from the observed frequencies.

To enable the estimation of ϱ the experimenter can, or when restricting to projective measurements even has to, determine relative frequencies of more than one POVM. This motivates the definition of a measurement scheme.

Definition 1 (Measurement scheme)**.** A tuple $M := (P_1, \ldots, P_l)$ of POVMs $P_i : 2^{I_i} \to \mathcal{L}(\mathcal{H}),\ i = 1, \ldots, l$, is called a measurement scheme on $\mathcal{H}$ of size l. The number of outcomes of M is $\sum_{i=1}^l |I_i|$.

The set of all measurement schemes on $\mathcal{H}$ is denoted by $MS_{\mathcal{H}}$. The complex span of all the effect operators $P_i(\{j\}),\ i = 1, \ldots, l,\ j = 1, \ldots, m_i$, of a measurement scheme $M := (P_1, \ldots, P_l) \in MS_{\mathcal{H}}$ is denoted by $\operatorname{Span} M$.

Proposition 6 (see Proposition 1 in [4])**.** *Let $\Sigma \subseteq \mathcal{L}(\mathcal{H})$ be a subspace. There is a measurement scheme $M \in MS_{\mathcal{H}}$ with $\operatorname{Span} M = \Sigma$ iff Σ is an operator system, i.e., iff $\Sigma^* = \Sigma$ and $\mathbb{1}_{\mathcal{H}} \in \Sigma$.*

Proof. Let $M \in MS_{\mathcal{H}}$ be such that $\operatorname{Span} M = \Sigma$. Then, by the definition of a measurement scheme, the subspace Σ is the complex span of self-adjoint operators and consequently $(\operatorname{Span} M)^* = \operatorname{Span} M$. Furthermore, by the normalization condition for POVMs, $\mathbb{1}_{\mathcal{H}} \in \Sigma$.

Conversely, assume Σ is an operator system of dimension $k \in \mathbb{N}$ and let $B_1, \ldots, B_k$ be a basis of Σ. Every $B_j,\ j = 1, \ldots, k$, can be decomposed as $B_j = X_j + iY_j$ with $X_j, Y_j \in H(\mathcal{H})$. As Σ is an operator system by assumption, it follows that $B_j^* \in \Sigma$ and hence $X_j, Y_j \in \Sigma,\ j = 1, \ldots, k$. Note that for every $j \in \{1, \ldots, k\}$ there are numbers $a_j, b_j \in \mathbb{R}$ such that $X_j' := a_j\mathbb{1}_{\mathcal{H}} + X_j$ and $Y_j' := b_j\mathbb{1}_{\mathcal{H}} + Y_j$ are positive and, as $\mathbb{1}_{\mathcal{H}} \in \Sigma$, both are elements of Σ. Finally, there are numbers $c_j, d_j \in \mathbb{R},\ j = 1, \ldots, k$, such that $Z := \mathbb{1}_{\mathcal{H}} - \sum_{j=1}^k (c_jX_j' + d_jY_j')$ is positive. Let $I := \{0, 1, \ldots, 2k\}$ and define a POVM $P : 2^I \to \mathcal{L}(\mathcal{H})$ by setting $P(0) = Z$, $P(j) = c_jX_j'$ for $j = 1, \ldots, k$ and $P(k + j) = d_jY_j'$ for $j = 1, \ldots, k$. Then, $M := (P)$ is a measurement scheme and $\operatorname{Span} M = \Sigma$. □

Remark 7. *Let Σ be an operator system. Given a POVM $P \in POVM_{\mathcal{H}}$ such that Span $P = \Sigma$, one can obtain a POVM $P' \in POVM_{\mathcal{H}}$ with* $\dim \Sigma$ *outcomes such that Span $P' = \Sigma$ by simply adding up redundant effect operators to one operator.*

In order for a measurement scheme $M := (P_1, \ldots, P_l) \in MS_{\mathcal{H}}$ to enable the tomography of any quantum state in $\mathcal{S}(\mathcal{H})$ it clearly has to be able to discriminate any two distinct quantum states when the sample size goes to infinity. In other words, there has to be a one-to-one correspondence between quantum states and the outcome distributions associated to measuring $P_1, \ldots, P_l$. This motivates the following definitions.

Definition 2 (Measurement map)**.** The measurement map D_P associated to a POVM $P \in POVM_{\mathcal{H}}$ is the linear map[1]

$$D_P : H(\mathcal{H}) \to \mathbb{R}^m,\ X \mapsto (\langle P(\{i\}), X\rangle_{HS})_{i=1}^m.$$

It maps a quantum state $\varrho \in \mathcal{S}(\mathcal{H})$ to its associated probability vector $D_P(\varrho) \in \mathbb{R}^m$ to which observed relative frequencies converge when the sample size goes to infinity. The measurement map D_M associated to a measurement scheme $M := (P_1, \ldots, P_l) \in MS_{\mathcal{H}}$ is the linear map defined by setting $D_M(X) := (D_{P_i}(X))_{i=1}^l$ for all $X \in H(\mathcal{H})$.

Definition 3 (Informationally complete)**.** A measurement scheme $M \in MS_{\mathcal{H}}$ is informationally complete iff the mapping $\mathcal{S}(\mathcal{H}) \ni \varrho \mapsto D_M(\varrho)$ is one-to-one, i.e., iff $D_M(\sigma) \neq D_M(\varrho)$ for all $\sigma, \varrho \in \mathcal{S}(\mathcal{H})$ with $\sigma \neq \varrho$.

Theorem 8. *Let $M := (P_1, \ldots, P_l) \in MS_{\mathcal{H}}$ be a measurement scheme and let $\Sigma_M :=$ Span $M \cap H(\mathcal{H})$. Then, the following are equivalent.*

1. *M is informationally complete,*
2. *D_M is injective,*
3. *$\Sigma_M = H(\mathcal{H})$.*

Proof. By definition of D_M one has Range $D_M^* = \Sigma_M$. Hence, the equivalence of 2. and 3. follows from the identity $(\text{Range}\, D_M^*)^\perp = \text{Ker}\, D_M$. It remains to be proven that 1. implies 2. as the converse clearly holds. Assume that M is informationally complete, i.e., that $D_M|_{S(\mathcal{H})}$ is injective. As by the normalization condition for POVMs on has $\mathbb{1}_{\mathcal{H}} \in \text{Range}\, D_M^*$, it suffices to show that $D_M|_{H_0}$ is injective, where $H_0 := \{X \in H(\mathcal{H}) : \text{tr}(X) = \langle \mathbb{1}_{\mathcal{H}}, X\rangle_{HS} = 0\}$. As $S(\mathcal{H})$ is a subset of the affine subspace $\{\frac{1}{n}\mathbb{1}_{\mathcal{H}} + X |\, X \in H_0\}$ with non-empty interior, $D_M|_{H_0}$ is injective by linearity of D_M. □

Remark 9. *In particular this result implies that if $M := (P_1, \ldots, P_l) \in MS_{\mathcal{H}}$ is an informationally complete measurement scheme the number of outcomes of M has to be greater or equal to $n^2 + l - 1$.*

[1] Recall that $H(\mathcal{H}) \subseteq \mathcal{L}(\mathcal{H})$ denotes the set of self-adjoint operators.

In view of the last theorem, a straightforward method to reconstruct quantum states from measurement data is linear inversion [47]. One issue of this approach is that an estimator obtained by means of linear inversion need not be a quantum state.

A common approach to recover an unknown quantum state from measurement data which avoids this problem is maximum likelihood estimation (MLE). When performing several experiments with an informationally complete measurement procedure $P := \{P_1, \ldots, P_m\} \in POVM_{\mathcal{H}}$ the MLE estimate of the true state $\varrho \in \mathcal{S}(\mathcal{H})$ is given by

$$\hat{\varrho} := \operatorname*{arg\,max}_{\sigma \in \mathcal{S}(\mathcal{H})} L(\sigma),$$

where $L(\sigma) := \prod_{i=1}^{m} \operatorname{tr}(P_i \sigma)^{f_i}$ is the likelihood function and $f_i,\ i = 1, \ldots, m$, is the observed frequency of the outcome i. Note that $\hat{\varrho}$ exists by the compactness of $\mathcal{S}(\mathcal{H})$ and continuity of L. Equivalently, minimizing the negative log-likelihood yields

$$\hat{\varrho} = \operatorname*{arg\,min}_{\sigma \in \mathcal{S}(\mathcal{H})} \left(-\log L(\sigma)\right) = \operatorname*{arg\,min}_{\sigma \in \mathcal{S}(\mathcal{H})} \sum_{i=1}^{m} -f_i \log\left(\operatorname{tr}(P_i \sigma)\right). \tag{2.1}$$

As the trace is linear and the negative logarithm is convex, the function $\mathcal{S}(\mathcal{H}) \ni \sigma \mapsto -\log L(\sigma)$ is a linear combination of convex functions and thus convex itself[1]. Hence, the MLE estimate $\hat{\varrho}$ is a minimizer of a convex optimization problem. Maximum likelihood techniques were for instance studied in [48, 49, 50, 51]. These techniques were also widely used in experiments (see, e.g., [52, 53, 54, 55, 56, 57]).

Apart from MLE, also Bayesian methods were proposed for estimation (see, e.g., [58, 59, 60, 61, 62, 63]). In practice, MLE often yields rank deficient estimates (see [63]). In scenarios where there is no prior information favouring low-rank quantum states, such an estimate might not be desirable. Bayesian methods do not suffer from this issue. They provide a full rank estimate together with a set of error bars. Other approaches with this feature are for instance the hedged maximum likelihood approach proposed in [64] or the approach taken in [65], where both the likelihood and the von Neumann entropy functionals are maximized. Furthermore, approaches to obtain confidence regions were proposed in [66, 67] which can yield very tight error bounds.

2.3 Quantum State Tomography under Prior Information

An experimenter might have some prior information about the preparation procedure he wants to identify by means of quantum state tomography. Mathematically, this prior information can

[1] Recall that $\mathcal{S}(\mathcal{H})$ is a convex set.

be represented in terms of the subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ of quantum states consistent with the prior. If the set $\mathcal{R}$ is of low dimensionality[1] as compared to the set $\mathcal{S}(\mathcal{H})$ of all quantum states, there are at least two ways in which one might be able to take advantage of the prior information: First, it might be possible to save measurement outcomes since quantum states in $\mathcal{R}$ might be uniquely determined among all other states in $\mathcal{R}$ by fewer outcomes as suggested by Remark 9. Second, it might be possible to reduce the sample complexity meaning that the number of quantum systems one has to prepare in order to get a good estimate of their quantum state might decrease. In the following, the focus is on the first option.

Definition 4 ($\mathcal{R}$-complete)**.** Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a subset. A measurement scheme $M \in MS_{\mathcal{H}}$ is $\mathcal{R}$-complete iff the mapping $\mathcal{R} \ni \varrho \mapsto D_M(\varrho)$ is injective. A POVM $P \in POVM_{\mathcal{H}}$ is $\mathcal{R}$-complete iff the measurement scheme $M = (P) \in MS_{\mathcal{H}}$ is $\mathcal{R}$-complete.

In order to perform a feasible tomography on a subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ with a measurement scheme $M \in MS_{\mathcal{H}}$, the scheme M clearly has to be $\mathcal{R}$-complete. The converse need not hold as the injectivity of $D_M|_{\mathcal{R}}$ does not imply the existence of a robust and computationally tractable recovery procedure required by a feasible tomography. In this section, the following question is studied: Given a subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$, what is the minimal number $m(\mathcal{R}) \in \mathbb{N}$ such that there exists an $\mathcal{R}$-complete measurement scheme $M \in MS_{\mathcal{H}}$ (or POVM $P \in POVM_{\mathcal{H}}$) with $m(\mathcal{R})$ outcomes? By the argument above, the minimal number of measurement outcomes needed to perform a robust and computationally tractable state tomography on the subset $\mathcal{R}$ could be greater than $m(\mathcal{R})$. However, it turns out that $m(\mathcal{R})$ can be a reasonable benchmark.

A different approach to the state discrimination problem for the special case of pure quantum states was considered in [68, 69]. Given a measurement scheme $M \in MS_{\mathcal{H}}$, the mapping $D_M|_{\mathcal{S}_1(\mathcal{H})}$ is not required to be injective, but rather injectivity is considered in a generic sense. In such a scenario far apart pure states might not be distinguishable and consequently there would be disjoint neighbourhoods of these states that have similar measurement outcomes. This might not be desirable regarding the stability of the tomography scheme.

2.3.1 Topological features

The following proposition shows that from a topological point of view measurement maps are well-behaved.

[1] The dimensionality could be measured for instance in terms of the Hausdorff dimension.

Proposition 10 (Proposition 6 of [4]). *If $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ is a closed subset and $M \in MS_{\mathcal{H}}$ is $\mathcal{R}$-complete, the mapping $D_M|_{\mathcal{R}}$ is a topological embedding, i.e., $D_M|_{\mathcal{R}}$ is a homeomorphism onto its image.*

Proof. The set $\mathcal{R}$ is compact as it is a closed subset of the compact set $\mathcal{S}(\mathcal{H})$. The map D_M is linear and hence continuous in the standard topologies. Consequently, the map $D_M|_{\mathcal{R}}$ is continuous when $\mathcal{R}$ is equipped with the induced topology. Finally, as M is $\mathcal{R}$-complete by assumption, the continuous map $D_M|_{\mathcal{R}}$ is injective and hence a homeomorphism onto its image by the compactness of $\mathcal{R}$. □

This proposition motivates the idea to not consider the specific structure of the mapping $D_M|_{\mathcal{R}}$, but to relax the initial question by asking for the minimal number $m_T(\mathcal{R}) \in \mathbb{N}$ such that the subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ can be embedded into Euclidean space of dimension $m_T(\mathcal{R})$ as a topological space. By Proposition 10, the number $m_T(\mathcal{R})$ is a lower bound on $m(\mathcal{R})$. Unfortunately, there is no general mathematical framework to deal with this rather general case. However, if $\mathcal{R}$ is a smooth manifold powerful tools based on algebraic topology are available. Therefore, the subsets of $\mathcal{S}(\mathcal{H})$ considered in the following are assumed to additionally come with a manifold structure.

Definition 5 (Immersion and embedding). Let $\mathcal{M}$ and $\mathcal{N}$ be smooth manifolds[1]. A smooth map $\psi : \mathcal{M} \to \mathcal{N}$ is an immersion iff the differential $d\psi_p : T_p\mathcal{M} \to T_{\psi(p)}\mathcal{N}$ is injective for all $p \in \mathcal{M}$ and a smooth embedding iff ψ is both an immersion and a homeomorphism onto its image.

A subset $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ is called (embedded) manifold iff there exists a manifold $\mathcal{M}$ and a smooth embedding $\psi : \mathcal{M} \to H(\mathcal{H})$ such that $\psi(\mathcal{M}) = \mathcal{P}$.

Definition 6 ($\mathcal{P}$-embedding). Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a manifold. A measurement scheme $M \in MS_{\mathcal{H}}$ is a $\mathcal{P}$-embedding iff $D_M|_{\mathcal{P}}$ is a smooth embedding. A POVM $P \in POVM_{\mathcal{H}}$ is a $\mathcal{P}$-embedding iff the measurement scheme $M = (P) \in MS_{\mathcal{H}}$ is a $\mathcal{P}$-embedding.

The question which can be approached with tools from algebraic topology is the following: Given a manifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$, what is the smallest number $m_I(\mathcal{P}) \in \mathbb{N}$ ($m_E(\mathcal{P}) \in \mathbb{N}$) such that there exists a smooth immersion $\psi : \mathcal{P} \to \mathbb{R}^{m_I(\mathcal{P})}$(embedding $\psi : \mathcal{P} \to \mathbb{R}^{m_E(\mathcal{P})}$)? The number $m_I(\mathcal{P})$ ($m_E(\mathcal{P})$) is called immersion (embedding) dimension. However, only in the case where $\mathcal{P}$-complete measurement schemes $M \in MS_{\mathcal{H}}$ are indeed $\mathcal{P}$-embeddings it is clear that these numbers are a lower bound on $m(\mathcal{P})$.

[1] Here, a smooth manifold is a second countable locally Euclidean Hausdorff topological space together with a smooth atlas. Smooth manifolds are assumed not to have boundaries.

The following lemma shows that the $\mathcal{R}$-complete and $\mathcal{R}$-embedding properties of a measurement scheme $M \in MS_{\mathcal{H}}$ solely depend on the operator system $\Sigma_M := \operatorname{Span} M$.

Lemma 11. *Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a subset and let $M \in MS_{\mathcal{H}}$ be a measurement scheme. Furthermore, denote by $\Pi_{\Sigma_M} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ the orthogonal projection on Σ_M.*

1. *The measurement scheme M is $\mathcal{R}$-complete iff $\Pi_{\Sigma_M}|_{\mathcal{R}}$ is injective.*
2. *If $\mathcal{R}$ is a closed manifold, the measurement scheme M is an $\mathcal{R}$-embedding iff $\Pi_{\Sigma_M}|_{\mathcal{R}}$ is a smooth embedding.*

Proof. By the definition of the map D_M, one has $\Sigma_M \cap H(\mathcal{H}) = \operatorname{Range} D_M^*$. Consequently, the map $\Pi_{\Sigma_M}|_{H(\mathcal{H})}$ is the orthogonal projection on the range of D_M^* and hence $\operatorname{Ker} \Pi_{\Sigma_M}|_{H(\mathcal{H})} = \operatorname{Ker} D_M$. Let $\varrho, \sigma \in \mathcal{R}$ with $\sigma \neq \varrho$ and assume M to be $\mathcal{R}$-complete. Then, $0 \neq D_M(\varrho) - D_M(\sigma) = D_M(\varrho - \sigma)$ and hence $\varrho - \sigma \notin \operatorname{Ker} D_M$. As $\operatorname{Ker} \Pi_{\Sigma_M}|_{H(\mathcal{H})} = \operatorname{Ker} D_M$, it follows that $0 \neq \Pi_{\Sigma_M}(\varrho - \sigma) = \Pi_{\Sigma_M}(\varrho) - \Pi_{\Sigma_M}(\sigma)$, i.e., $\Pi_{\Sigma_M}|_{\mathcal{R}}$ is injective. The converse direction can be proven similarly.

Now assume $\mathcal{R}$ to be a closed manifold. Note that $d(D_M|_{\mathcal{R}})_\varrho = D_M|_{T_\varrho \mathcal{R}}$ for all $\varrho \in \mathcal{R}$ by linearity of D_M and similarly $d(\Pi_{\Sigma_M}|_{\mathcal{R}})_\varrho = \Pi_{\Sigma_M}|_{T_\varrho \mathcal{R}}$. Assuming M to be an $\mathcal{R}$-embedding, the map $D_M|_{\mathcal{R}}$ is an immersion. By linearity of D_M this is equivalent to $T_\varrho \mathcal{R} \cap \operatorname{Ker} D_M = \emptyset$ for all $\varrho \in \mathcal{R}$. As $\operatorname{Ker} \Pi_{\Sigma_M}|_{H(\mathcal{H})} = \operatorname{Ker} D_M$ it follows that $\Pi_{\Sigma_M}|_{\mathcal{R}}$ is an immersion. Since $D_M|_{\mathcal{R}}$ is injective by assumption, by 1. the map $\Pi_{\Sigma_M}|_{\mathcal{R}}$ is injective. As $\Pi_{\Sigma_M}|_{\mathcal{R}}$ is continuous and injective, it is a homeomorphism onto its image by the compactness of $\mathcal{R}$. Again, the converse can be proven similarly. □

Remark 12. *With respect to the $\mathcal{R}$-complete and $\mathcal{R}$-embedding properties two measurement schemes $M_1, M_2 \in MS_{\mathcal{H}}$ are thus equivalent, written as $M_1 \sim M_2$, if $\operatorname{Span} M_1 = \operatorname{Span} M_2$. Hence, for each POVM $P := \{P_1, \ldots, P_m\} \in POVM_{\mathcal{H}}$ one can define an equivalent collection of binary measurement settings by $M_b := (\{P_i, \mathbb{1}_{\mathcal{H}} - P_i\})_{i=1}^m \sim (P)$.*

2.3.2 The Immersion Dimension

To illustrate how methods from algebraic topology can be utilized to lower bound the immersion dimension of a manifold, a particular method based on Stiefel-Whitney classes is presented in this section. A regular homotopy of immersions is a homotopy such that each map in the deformation process is an immersion. Hirsch-Smale theory is the study of regular homotopy classes of immersions. In this framework, Hirsch [70] proved the following result showing that the existence of an immersion of a manifold into Euclidean space is equivalent to a vector bundle equation.

Theorem 13 (Hirsch)**.** *Let $\mathcal{M}$ be a d-dimensional compact manifold. There exists an immersion of the manifold $\mathcal{M}$ into $\mathbb{R}^{d+k}$ iff there exists a rank k vector bundle $N\mathcal{M}$ on $\mathcal{M}$ such that the*

sum of $N\mathcal{M}$ with the tangent bundle $T\mathcal{M}$ is trivial, i.e.,

$$T\mathcal{M} \oplus N\mathcal{M} = \xi_{d+k},$$

where ξ_{d+k} denotes the trivial bundle on $\mathcal{M}$ of rank $d+k$.

In the previous theorem the bundle $N\mathcal{M}$ can be interpreted as a normal bundle on $\mathcal{M}$. If $\mathcal{M}$ is a d-dimensional compact smooth manifold that can be embedded into Euclidean space of dimension $d+k$, the vector bundle equation

$$T\mathcal{M} \oplus N\mathcal{M} = \xi_{d+k} \tag{2.2}$$

can be used to lower bound the immersion dimension of $\mathcal{M}$. For instance, this can be achieved by means of Stiefel-Whitney classes (see, e.g., Chapter 4 of [71] or Chapter 3 of [72] for an introduction to Stiefel-Whitney classes): Denote by $H^*(\mathcal{M};\mathbb{Z}_2)$ the cohomology ring of the manifold $\mathcal{M}$ with coefficients in $\mathbb{Z}_2$ and by $\smile$ the cup product. The total Stiefel-Whitney class of a vector bundle V on a compact smooth manifold $\mathcal{M}$ is denoted by $\omega(V) \in H^*(\mathcal{M};\mathbb{Z}_2)$. As the Stiefel Whitney class of a direct sum of vector bundles is the cup product of the summands' Stiefel Whitney classes (see Theorem 3.1 of [72]), one obtains

$$\omega(T\mathcal{M} \oplus N\mathcal{M}) = \omega(T\mathcal{M}) \smile \omega(N\mathcal{M}).$$

Using Equation 2.2 and the fact that $\omega(\xi_{d+k}) = 1$ (see Proposition 2 in Chapter 4 of [71]), this yields

$$\begin{aligned} &\omega(T\mathcal{M}) \smile \omega(N\mathcal{M}) = 1 \\ \Leftrightarrow &\omega(N\mathcal{M}) = \overline{\omega(T\mathcal{M})}, \end{aligned} \tag{2.3}$$

where $\overline{\omega(T\mathcal{M})}$ denotes the inverse of $\omega(T\mathcal{M})$. From this, one can obtain the following non-immersion result (see, e.g., Chapter 4 of [71]).

Proposition 14. *Let $\mathcal{M}$ be a compact smooth manifold of dimension d. Let $k \in \mathbb{N}$ be the largest integer such that $\overline{\omega(T\mathcal{M})}_k \neq 0$. Then, the manifold $\mathcal{M}$ cannot be immersed in Euclidean space of dimension $d+k-1$, i.e., $m_I(\mathcal{M}) \geq d+k$.*

Proof. Assume $\mathcal{M}$ could be immersed in Euclidean space of dimension $d+k-1$. Then, by Theorem 13, there exists a bundle $N\mathcal{M}$ on $\mathcal{M}$ of rank $k-1$ such that $T\mathcal{M} \oplus N\mathcal{M} = \xi_{d+k-1}$. By Theorem 3.1 of [72], it holds that $\omega(N\mathcal{M})_i = 0$ for $i > \operatorname{rank} N\mathcal{M} = k-1$. In particular this yields $\omega(N\mathcal{M})_k = 0$. Using Equation (2.3) this yields $\overline{\omega(T\mathcal{M})}_k = 0$, a contradiction. □

This illustrates one way to obtain non-immersion results from topological invariants. The non-immersion results for complex flag manifolds which are used in Article I are based on the integrality theorem given in [5].

2.3.3 Pure Quantum States as an Example

In this section, it is demonstrated how non-embedding respectively non-immersion results can be used to lower bound the number of measurement outcomes required to discriminate any two pure states. It is first shown that a measurement scheme which can discriminate any two pure states gives rise to a smooth embedding of the set of pure states $\mathcal{S}_1(\mathcal{H})$ into Euclidean space. This result is a consequence of Theorem 5 and Lemma 1 of [4].

Lemma 15. *Let $M \in MS_{\mathcal{H}}$ be an $\mathcal{S}_1(\mathcal{H})$-complete measurement scheme. Then, M is an $\mathcal{S}_1(\mathcal{H})$-embedding.*

Proof. By Proposition 10, the map $D_M|_{\mathcal{S}_1(\mathcal{H})}$ is a topological embedding. It remains to be shown that $D_M|_{\mathcal{S}_1(\mathcal{H})}$ is an immersion.

First, as $D_M|_{\mathcal{S}_1(\mathcal{H})}$ is injective, it follows that if $D_M(X) = 0$ for an $X \in \Delta(\mathcal{S}_1(\mathcal{H})) := \{\lambda(\varrho_1 - \varrho_2) : \varrho_1, \varrho_2 \in \mathcal{S}_1(\mathcal{H}), \lambda \in \mathbb{R}_+\}$ then one has $X = 0$, because otherwise there would exist $\varrho_1, \varrho_2 \in \mathcal{S}_1(\mathcal{H})$ and $\lambda > 0$ such that $X = \lambda(\varrho_1 - \varrho_2)$ and hence $0 = D(X) = D(\lambda(\varrho_1 - \varrho_2)) = \lambda(D(\varrho_1) - D(\varrho_2))$, a contradiction.

Let $\varrho \in \mathcal{S}_1(\mathcal{H})$ be arbitrary. By the linearity of D_M, it follows that $d(D_M|_{\mathcal{S}_1(\mathcal{H})})_\varrho = D_M|_{T_\varrho \mathcal{S}_1(\mathcal{H})}$. In order to prove the injectivity of the linear map $D_M|_{T_\varrho \mathcal{S}_1(\mathcal{H})}$, by the above argument it suffices to show that $T_\varrho \mathcal{S}_1(\mathcal{H}) \subseteq \Delta(\mathcal{S}_1(\mathcal{H}))$.

Consider the smooth curve $\gamma_H : \mathbb{R} \to \mathcal{S}_1(\mathcal{H}),\ t \mapsto e^{iHt}\varrho e^{-iHt}$, where $H \in H(\mathcal{H})$ is self-adjoint. Then, one has (see, e.g., the proof of Lemma 1 in [4])

$$T_\varrho \mathcal{S}_1(\mathcal{H}) = \left\{ \frac{d}{dt}\gamma_H(0) = i(H\varrho - \varrho H) :\ H \in H(\mathcal{H}) \right\}.$$

Since ϱ is rank one, the commutator $i[H, \varrho] := i(H\varrho - \varrho H)$, $H \in H(\mathcal{H})$, is the difference of two operators of rank at most one. Consequently, $i[H, \varrho]$ is a self-adjoint operator of rank at most two for all $H \in H(\mathcal{H})$. As $\mathrm{tr}(i[H, \varrho]) = 0$, it follows that $i[H, \varrho]$ either has precisely two nonzero eigenvalues with equal magnitude and opposite sign or is equal to zero. It suffices to show that every traceless rank two self-adjoint operator $X \in H(\mathcal{H})$ is proportional to the difference of two rank one projections $\varrho_1, \varrho_2 \in \mathcal{S}_1(\mathcal{H})$. As every such X has precisely two nonzero eigenvalues with equal magnitude and opposite sign, this follows from the spectral theorem. □

The set of pure states $\mathcal{S}_1(\mathcal{H})$ can be identified with the complex projective space $P(\mathcal{H}) \simeq P\mathbb{C}^{n-1}$. Indeed, the map $\psi : P(\mathcal{H}) \to H(\mathcal{H}),\ [v] \mapsto vv^*/\|v\|$ is a smooth embedding. Consequently, if $M \in MS_{\mathcal{H}}$ is $\mathcal{S}_1(\mathcal{H})$-complete, the map $D_M \circ \psi$ is a smooth embedding of a complex projective space into Euclidean space by Lemma 15. It follows that the embedding dimension of $P\mathbb{C}^{n-1}$ lower bounds the number of measurement outcomes needed to discriminate any two

pure states, i.e.[1],

$$m(\mathcal{S}_1(\mathcal{H})) \geq m_E(P\mathbb{C}^{n-1}) + 1.$$

As a result, the lower bounds on $m_E(P\mathbb{C}^{n-1})$ given in [5] yield lower bounds on $m(\mathcal{S}_1(\mathcal{H}))$.

Theorem 16 (Section 4.6 of [5])**.** *It holds that*

$$m_E(P\mathbb{C}^{n-1}) > \begin{cases} 4n-4-2\alpha(n-1) & \forall n > 1 \\ 4n-4-2\alpha(n-1)+1 & \text{for } n \text{ odd and } \alpha(n-1) = 2 \, mod 4 \\ 4n-4-2\alpha(n-1)+2 & \text{for } n \text{ odd and } \alpha(n-1) = 3 \, mod 4, \end{cases}$$

where $\alpha(k)$ is the number of ones in the dyadic expansion of $k \in \mathbb{N}$.

As $\alpha(n) = \mathcal{O}(\log n)$, this bound is essentially determined by the $4n$ term. Explicit constructions of embeddings of complex projective space into Euclidean space given in [6] show that the lower bounds of Theorem 16 are close to optimal. Fortunately, the construction given in [6] yields an explicit set of self-adjoint operators $\{A_i\}_{i\in I} \subseteq H(\mathcal{H})$ such that the linear map $H(\mathcal{H}) \ni X \mapsto (\mathrm{tr}(A_i X))_{i\in I}$ can discriminate any two pure states (for more details, see the proof of Theorem 4 in [4]). Consequently, the subspace $\Sigma := \mathrm{Span}\,\{A_i\}_{i\in I} \cup \{\mathbb{1}_{\mathcal{H}}\}$ is an operator system and by Proposition 6 and Remark 7, there exists a POVM with $\dim \Sigma$ outcomes such that $\mathrm{Span}\, P = \Sigma$. As a result, the construction given in [6] gives rise to $\mathcal{S}_1(\mathcal{H})$-complete POVMs and therefore also yields strong upper bounds on the number $m(\mathcal{S}_1(\mathcal{H}))$.

Theorem 17 (Theorem 3 of [4])**.** *There exists an $\mathcal{S}_1(\mathcal{H})$-complete POVM $P \in POVM_{\mathcal{H}}$ with*

$$m = 1 + \begin{cases} 4n-4-\alpha(n-1) & \text{for even } n \\ 4n-4-\alpha(n-1)+1 & \text{for odd } n \end{cases}$$

outcomes.

Next, pure state tomography by means of von Neumann measurements is considered. It follows from Theorem 16 that in dimensions greater than four at least four von Neumann measurements are required to discriminate any two pure states. Using Hermite polynomials, an $\mathcal{S}_1(\mathcal{H})$-complete measurement scheme consisting of four von Neumann measurements is explicitly constructed in [8] showing that the lower bound is tight for dimensions greater than four.

Definition 7 (Orthogonal polynomials)**.** A sequence of univariate real polynomials $(p_n)_{n\in\mathbb{N}_0}$ is called a sequence of orthogonal polynomials iff the following two condictions hold:

[1] Because of the normalization condition for POVMs there is one redundant outcome and therefore the lower bound is not $m_E(P\mathbb{C}^{n-1})$ but $m_E(P\mathbb{C}^{n-1}) + 1$.

1. p_n is of degree n for every $n \in \mathbb{N}_0$.
2. There exists a Borel measure μ with $\int_{\mathbb{R}} |x|^n d\mu(x) < \infty$ for all $n \in \mathbb{N}_0$ such that $\langle p_n, p_m \rangle := \int_{\mathbb{R}} p_n(x) p_m(x) d\mu(x) = 0$ for all $n, m \in \mathbb{N}$ with $n \neq m$.

In Section 5 of [9], the construction given in [8] was generalized to arbitrary sequences of orthogonal polynomials yielding the following result.

Theorem 18 (Section 5 of [9])**.** *Let $(p_n)_{n\in\mathbb{N}}$ be a sequence of orthogonal polynomials. Furthermore, let $x_0, \ldots, x_{n-1}$ and $y_0, \ldots, y_{n-2}$ be the zeros of the polynomials p_n and p_{n-1} respectively. For $i = 0, \ldots, n-1$ define the vectors*

$$v_i^1 := (p_0(x_j), p_1(x_j), \ldots, p_{n-1}(x_j)),$$
$$v_i^2 := (p_0(x_j), e^{i\pi/n} p_1(x_j), \ldots, e^{i(n-1)\pi/n} p_{n-1}(x_j)).$$

For $i = 0, \ldots, n-2$ define the vectors

$$v_i^3 := (p_0(y_j), p_1(y_j), \ldots, p_{n-2}(y_j), 0),$$
$$v_i^4 := (p_0(y_j), e^{i\pi/n} p_1(y_j), \ldots, e^{i(n-2)\pi/n} p_{n-2}(y_j), 0)$$

and set $v_{n-1}^3 := (0, \ldots, 0, 1)$ as well as $v_{n-1}^4 := (0, \ldots, 0, 1)$. Then,

$$P^l := \{v_j^l (v_j^l)^* / \|v_j^l\|^2 \,|\, j = 0, \ldots, n-1\},\ l = 1, 2, 3, 4,$$

are von Neumann measurements and the measurement scheme $M := (P^l)_{l=1}^4$ is $\mathcal{S}_1(\mathbb{C}^n)$-complete.

In [7] it is shown that Haar almost all collections of four von Neumann measurements on $\mathbb{C}^n$ are $\mathcal{S}_1(\mathbb{C}^n)$-complete.

The results presented above are concerned with measurements which can separate any two pure states. A stronger separability property was considered in [21, 73]. These articles analyze measurement schemes which can discriminate pure states from arbitrary states, i.e., measurements schemes $M \in MS_{\mathcal{H}}$ such that if $M(\varrho) = M(\sigma)$ holds for some $\varrho \in \mathcal{S}_1(\mathcal{H})$ and $\sigma \in \mathcal{S}(\mathcal{H})$ then $\varrho = \sigma$. Geometrically, this means that the affine space $\{M(\varrho) + X \,|\, X \in \operatorname{Ker} M\}$ is a separating hyperplane in the sense that it intersects the set $\mathcal{S}(\mathcal{H})$ in precisely the point ϱ. This property is crucial for the analysis given in the articles III and V.

2.3.4 Whitney Embedding Theorem

In this section, a general upper bound on the number $m(\mathcal{R})$ is presented which depends solely on the dimension of the subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$. It straightforwardly follows from the basic version of the Whitney embedding theorem (see, e.g., Section 8 in Chapter 1 of [41]).

Theorem 19. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a closed manifold. Then, there exists a $\mathcal{P}$-embedding $P \in POVM_{\mathcal{H}}$ with $2\dim\mathcal{P}+2$ outcomes.*

Proof. As $\mathcal{P}$ is an embedded manifold, there exists a smooth manifold $\mathcal{M}$ and a smooth embedding $\psi : \mathcal{M} \mapsto H(\mathcal{H})$ with $\psi(\mathcal{M}) = \mathcal{P}$. Let $k := \dim\mathcal{M}$.

First, the following claim is proven: Let $L : H(\mathcal{H}) \to \mathbb{R}^m$ be linear map such that $L \circ \psi$ is an injective immersion. If $m > 2k+1$, there exists a vector $v \in \mathbb{R}^m$ such that $\Pi_v \circ L \circ \psi$ is an injective immersion, where Π_v is the orthogonal projection on $S := \{w \in \mathbb{R}^m | \langle w, v\rangle = 0\}$.

In order to prove this, let $g : T\mathcal{M} \to \mathbb{R}^m$, $(x,v) \mapsto L \circ d_x\psi(v)$ and $f : \mathcal{M}\times\mathcal{M}\times\mathbb{R}_+ \to (x,y,\lambda) \mapsto \lambda((L\circ\psi)(x) - (L\circ\psi)(y))$. Both f and g are smooth and as $\dim(\mathcal{M}\times\mathcal{M}\times\mathbb{R}_+) = 2k+1 < m$ and $\dim(T\mathcal{M}) = 2k < m$, there is a point $v \in \mathbb{R}^m$ that is neither in the image of f nor in the image of g (this is a consequence of Sard's theorem, see for instance Section 7 in Chapter 1 of [41]). Furthermore, one has $v \neq 0$ as 0 is contained in both the images of f and g. The vector v has the desired property: Suppose that $(\Pi_v \circ L \circ \psi)(x) = (\Pi_v \circ L \circ \psi)(y)$ for some $x, y \in \mathcal{M}$ with $x \neq y$. It follows that $\Pi_v((L\circ\psi)(x) - (L\circ\psi)(y)) = 0$. Consequently, $(L\circ\psi)(x) - (L\circ\psi)(y) = \lambda v$ for some $\lambda \in \mathbb{R}$. As $L\circ\psi$ is injective and $x \neq y$, one has $\lambda \neq 0$. Therefore, one has $f(x,y,1/\lambda) = v$, contradicting the choice of v. Similarly, suppose $d(\Pi_v \circ L \circ \psi)_x(w) = \Pi_v \circ L \circ d_x\psi(w) = 0$ for some $(x,w) \in T\mathcal{M}$ with $w \neq 0$. By the definition of Π_v and the injectivity of $d\psi_x$, it follows that $\lambda v = L \circ d\psi_x(w)$ for some $\lambda \neq 0$. Consequently, $g(x, 1/\lambda w) = v$, contradicting the choice of v.

This shows that there exists a linear map $L : H(\mathcal{H}) \to \mathbb{R}^{2k+1}$ such that $L\circ\psi$ is an injective immersion[1]. The manifold $\mathcal{P}$ is compact as it is a closed subset of a compact set. Consequently, the map $L\circ\psi$ is a smooth embedding.

By Proposition 6 and Remark 7 there exists a POVM $P \in POVM_{\mathcal{H}}$ with $2k+2$ outcomes such that $\operatorname{Range} L^* \subseteq \operatorname{Span} P$. Finally, Lemma 11 concludes the proof. □

Remark 20. *Note that the strength of this result essentially depends on the dimensions of $\Delta(\mathcal{P}) := f(\mathcal{M}\times\mathcal{M}\times\mathbb{R}_+)$ and $g(T\mathcal{M})$ rather than the dimension of $\mathcal{P}$. The result was obtained by means of the estimates $\dim\Delta(\mathcal{P}) \leq 2\dim\mathcal{P}+1$ and $\dim g(T\mathcal{M}) \leq 2\dim\mathcal{P}$. Hence, given a specific manifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$, this proof strategy leaves room for improvement.*

In the context of the phase retrieval problem, a conceptually similar approach was used in [10] to find intensity measurements which can discriminate any two signals up to a phase. However, they consider the problem in the framework of semi-algebraic geometry rather than smooth manifold theory. As it comes with a rich dimension theory, semi-algebraic geometry allows for a stronger and more flexible argument. The articles II, IV, VI make use of this approach. The flexibility of algebraic geometry methods in particular facilitate the analysis of constrained measurements schemes such as von Neumann measurements.

[1] Identifying $H(\mathcal{H})$ with $\mathbb{R}^{n^2}$, one can start the argument given above with the identity map and inductively apply it until on obtains the desired map L.

The dimension argument is the crucial step in the proof of Theorem 19 and a similar theorem, called Mané's Theorem (see [74, 75]), can be proven for the Hausdorff dimension. Mané's Theorem states that for an arbitrary compact set $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ almost any linear map (in a Lebesgue measure sense) $L : H(\mathcal{H}) \to \mathbb{R}^m$ is injective when restricted to $\mathcal{R}$ if m is strictly larger than twice the Hausdorff dimension of $\mathcal{R}$.

2.4 Feasible Tomography of Low-Rank Quantum States

In this section, a computationally tractable recovery procedure for low-rank quantum states based on techniques from compressed sensing is presented (see [2, 3, 37, 38]). This procedure has also been experimentally tested [76].

Throughout this section, let $\mathcal{H} = (\mathbb{C}^2)^{\otimes d}$. The set of Pauli observables on $\mathcal{H}$ is given by

$$PO_{\mathcal{H}} := \{\sigma_1 \otimes \ldots \otimes \sigma_d | \, \forall i \in \{1, \ldots, d\} : \sigma_i \in \{\mathbb{1}, \sigma^x, \sigma^y, \sigma^z\}\},$$

where $\sigma^x, \sigma^y, \sigma^z \in H(\mathbb{C}^2)$ are the standard Pauli operators. Let A be a discrete, uniformly distributed, operator-valued random variable with range $PO_{\mathcal{H}}$ and let $\mathcal{A}_1, \ldots, \mathcal{A}_m$ be be independent realizations of A, i.e., with replacement samples of $PO_{\mathcal{H}}$[1]. Define the measurement map D as

$$D : H(\mathcal{H}) \ni X \mapsto (\mathrm{tr}(\mathcal{A}_i X))_{i=1}^m.$$

The measurement map D is associated to the following measurement procedure: First, take m independent realizations $\mathcal{A}_1, \ldots, \mathcal{A}_m$ of the random variable A. Then estimate the expectation values $\mathrm{tr}(\mathcal{A}_i \varrho), \; i \in \{1, \ldots, m\}$, in a statistical experiment, where $\varrho \in \mathcal{S}(\mathcal{H})$ is the state to be measured. More precisely, given k quantum systems prepared in state ϱ, for each $i \in \{1, \ldots, m\}$ take k/m of these systems, measure the observable $\mathcal{A}_i$ on each of the k/m systems and average the observed outcomes to obtain an estimate of $\mathrm{tr}(\mathcal{A}_i \varrho)$. In the following, the resulting estimate of $D(\varrho)$ is denoted by $\hat{D}(\varrho)$.

The result of this tomography scheme is given by

$$\tilde{b} := \hat{D}(\varrho) = D(\varrho) + \sqrt{\frac{m}{n}} z,$$

where $z \in \mathbb{R}^m$ is an error term accounting for statistical noise caused by the finite sample size, or more generally for all sources of error the measurement procedure is exposed to.

[1] The main reason to sample with replacement is that i.i.d. random variables considerably simplify the analysis.

Motivated by results in matrix recovery (see [16, 17, 77]), the idea presented in [2, 3] is to utilize this probabilistic measurement procedure for the tomography of bounded rank quantum states. It is shown that an unknown state of rank at most r can be reconstructed with high probability from $m = \mathcal{O}(rn \log^2 n)$ expectations of randomly sampled Pauli observables. The reconstruction can be implemented by means of a semidefinite program (SDP) and hence is computationally tractable (see, e.g., [78, 79, 80, 81] for solvers). The articles III and V deploy essentially the same convex programs for the recovery.

In the remainder of this section, the similar yet technically different approach taken in [37, 38] is presented in somewhat more detail.

In the absence of noise, an intuitive approach for reconstructing low-rank quantum states from measurement outcomes is the following: Let $\sigma \in \mathcal{S}_r(\mathcal{H})$ be the unknown quantum state. Among all quantum states $\varrho \in \mathcal{S}(\mathcal{H})$ which are consistent with the measurement outcomes, i.e., $D(\varrho) = D(\sigma)$, choose the one with the smallest rank. In case D can discriminate any two quantum states of rank at most r, there is indeed only one such state. However, as rank minimization is NP-hard in general [82], this approach is not computationally feasible. With the intuition that the trace norm is a good convex surrogate for the rank function, the following two estimators can be understood as convex relaxations of this approach. To simplify notation in the following, define

$$\mathcal{D} := \sqrt{\frac{n}{m}} D,$$
$$b := \sqrt{\frac{n}{m}} \tilde{b}.$$

The first estimator, known as the matrix Dantzig selector, is obtained by constrained trace norm minimization:

$$\hat{\varrho}_D := \operatorname*{arg\,min}_{X \in H(\mathcal{H}), \|\mathcal{D}^*(\mathcal{D}(X) - b)\|_\infty \leq \lambda} \|X\|_1, \tag{2.4}$$

where $\lambda > 0$ is an error scale that has to be chosen in advance and $\|\cdot\|_\infty$,$\|\cdot\|_1$ denote the Schatten ∞-norm and the trace norm, respectively. The second estimator, known as the matrix Lasso, is obtained by least squares regularized with the trace norm:

$$\hat{\varrho}_L := \operatorname*{arg\,min}_{X \in H(\mathcal{H})} \frac{1}{2} \|\mathcal{D}(X) - b\|^2 + \mu \|X\|_1, \tag{2.5}$$

where again $\mu > 0$ is a constant that has to be chosen in advance.

One approach to prove recovery guarantees for these estimators is by means of the restricted isometry property (RIP) [16].

Definition 8 (RIP)**.** A linear map $\mathcal{D} : H(\mathcal{H}) \to \mathbb{R}^m$ satisfies the restricted isometry property with distortion $0 \leq \delta < 1$ over $\mathcal{R} \subseteq H(\mathcal{H})$ iff

$$(1-\delta)\|X\|_{HS} \leq \|\mathcal{D}(X)\| \leq (1+\delta)\|X\|_{HS}$$

holds for all $X \in \mathcal{R}$.

Theorem 21 (Theorem 2.1 of [37])**.** *Let $\delta \in [0,1)$. If $m = Crn\log^6 n$, then, with probability $1-p$, the linear map $\mathcal{D}$ satisfies the RIP over $\mathcal{S}_r(\mathcal{H})$ with distortion δ, where C is a constant which only depends on δ and $C = \mathcal{O}(1/\delta^2)$. The probability of failure p is exponentially small in $\delta^2 C$.*

This result shows that $\mathcal{S}_r(\mathcal{H})$ can be embedded in Euclidean space of dimension $m = \mathcal{O}(rn\log^6 n)$ with only little distortion.

In the following, a quantum state $\varrho \in \mathcal{S}(\mathcal{H})$ is decomposed as $\varrho = \varrho_r + \varrho_c$, where $\varrho_r \in \mathcal{S}_r(\mathcal{H})$ is the best rank r approximation to ϱ and ϱ_c is the residual part. Combining Theorem 21 with Lemma 3.2 of [83] yields strong error bounds for the estimators (2.4) and (2.5).

Theorem 22 (Theorem 1 of [38])**.** *Let $m = Crn\log^6 n$, where C is an appropriate absolute constant. Then, there exist absolute constants $C_1, C_2, C_1', C_2' > 0$ such that the following statements hold with high probability over the choice of D:*

1. *Assume the noise $z \sim \mathcal{N}(0, \sigma\mathbb{1})$ is a Gaussian random vector. Choose $\lambda > 0$ such that $\lambda \geq \|\mathcal{D}^*(z)\|_\infty$. Let $\varrho = \varrho_r + \varrho_c \in \mathcal{S}(\mathcal{H})$ be any quantum state and let $\hat{\varrho}_D$ be the Dantzig selector* (2.4)*. Then, the inequality*

$$\|\hat{\varrho}_{DS} - \varrho\|_1 \leq C_1 r\lambda + C_2\|\varrho_c\|_1$$

holds with high probability over the Gaussian noise z.

2. *Assume the noise $z \sim \mathcal{N}(0, \sigma\mathbb{1})$ is a Gaussian random vector. Choose $\mu > 0$ such that $\mu/2 \geq \|\mathcal{D}^*(z)\|_\infty$. Let $\varrho = \varrho_r + \varrho_c \in \mathcal{S}(\mathcal{H})$ be any quantum state and let $\hat{\varrho}_L$ be the Lasso* (2.5)*. Then, the inequality*

$$\|\hat{\varrho}_L - \varrho\|_1 \leq C_1' r\mu + C_2'\|\varrho_c\|_1$$

holds with high probability over the noise z.

Remark 23. *As opposed to the dual certificate approach taken in [2, 3], the analysis based on the RIP comes with uniform recovery guarantees and stronger error bounds. However, the number m of required measurements exceeds the ones given in [2, 3] by a $\operatorname{poly}\log n$ factor.*

The first term in the error bound accounts for the statistical noise and is sensitive to the sample size. The second term is determined by the tail ϱ_c and hence can account for imperfect prior information.

Finally, the sample complexity of the tomography scheme introduced above can also be estimated.

Theorem 24 (Theorem 2 of [38]). *Let $m = Crn\log^6 n$, where C is an appropriate absolute constant. Let $\epsilon > 0$ and assume the sample size satisfies $t = \mathcal{O}\left(\left(\frac{nr}{\epsilon}\right)^2 \log n\right)$. Then, the following statements hold with high probability over the choice of D:*

1. *Choose $\lambda = \frac{\epsilon}{C_1 r}$. Let $\varrho = \varrho_r + \varrho_c \in \mathcal{S}(\mathcal{H})$ be any quantum state and let $\hat{\varrho}_D$ be the Dantzig selector* (2.4). *Then, the inequality*

$$\|\hat{\varrho}_L - \varrho\|_1 \leq \epsilon + C_2\|\varrho_c\|_1$$

   holds with high probability over the measurement data.

2. *Choose $\lambda = \frac{\epsilon}{C_1' r}$. Let $\varrho = \varrho_r + \varrho_c \in \mathcal{S}(\mathcal{H})$ be any quantum state and let $\hat{\varrho}_L$ be the Lasso* (2.5). *Then, the inequality*

$$\|\hat{\varrho}_L - \varrho\|_1 \leq \epsilon + C_2\|\varrho_c\|_1$$

   holds with high probability over the measurement data.

By Theorem 4 of [38], this result is nearly optimal in the sense that when using this tomography scheme, the number of samples t has to grow at least as fast as $\mathcal{O}(\frac{n^2r^2}{\log n})$ to achieve a constant size confidence interval in trace norm for all rank r states.

The sample complexity of more general tomography schemes is analyzed in [84]. The authors show that $\mathcal{O}(nr\log n)$ samples suffice in order to achieve a constant size confidence interval in trace norm and also prove that this result is nearly optimal.

Bibliography

[1] H Häffner, W Hänsel, CF Roos, J Benhelm, et al. **Scalable multiparticle entanglement of trapped ions**. *Nature*, **438**(7068):643–646, 2005. 1

[2] David Gross, Yi-Kai Liu, Steven T Flammia, Stephen Becker, and Jens Eisert. **Quantum state tomography via compressed sensing**. *Physical review letters*, **105**(15):150401, 2010. 2, 8, 12, 28, 29, 30

[3] David Gross. **Recovering low-rank matrices from few coefficients in any basis**. *IEEE Trans. on Information Theory*, **57**:1548–1566, 2011. 2, 8, 12, 28, 29, 30

[4] Teiko Heinosaari, Luca Mazzarella, and Michael M Wolf. **Quantum tomography under prior information**. *Communications in Mathematical Physics*, **318**(2):355–374, 2013. 3, 12, 17, 21, 24, 25

[5] Karl Heinz Mayer. **Elliptische Differentialoperatoren und Ganzzahligkeitssätze für charakteristische Zahlen**. *Topology*, **4**(3):295–313, 1965. 3, 23, 25

[6] R James Milgram. **Immersing projective spaces**. *The Annals of Mathematics*, **85**(3):473–482, 1967. 3, 25

[7] Damien Mondragon and Vladislav Voroninski. **Determination of all pure quantum states from a minimal number of observables**. *arXiv preprint arXiv:1306.1214*, 2013. 5, 26

[8] Philippe Jaming. **Uniqueness results in an extension of Pauli's phase retrieval problem**. *Applied and Computational Harmonic Analysis*, **37**(3):413–441, 2014. 5, 8, 25, 26

[9] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. **How many orthonormal bases are needed to distinguish all pure quantum states?** *The European Physical Journal D*, **69**(7):1–11, 2015. 5, 26

[10] Radu Balan, Pete Casazza, and Dan Edidin. **On signal reconstruction without phase**. *Applied and Computational Harmonic Analysis*, **20**(3):345–356, 2006. 5, 27

[11] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. **An algebraic characterization of injectivity in phase retrieval**. *Applied and Computational Harmonic Analysis*, 2014. 5

[12] Richard Kueng, Holger Rauhut, and Ulrich Terstiege. **Low rank matrix recovery from rank one measurements**. *Applied and Computational Harmonic Analysis*, 2015. 5

[13] Dan Edidin. **Projections and phase retrieval**. *Applied and Computational Harmonic Analysis*, 2015. 5

[14] Cynthia Vinzant. **A small frame and a certificate of its injectivity**. *arXiv preprint arXiv:1502.04656*, 2015. 5

[15] Zhiqiang Xu. **The minimal measurement number for low-rank matrices recovery**. *arXiv preprint arXiv:1505.07204*, 2015. 5

[16] Benjamin Recht, Maryam Fazel, and Pablo A Parrilo. **Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization**. *SIAM review*, **52**(3):471–501, 2010. 6, 12, 29

[17] Emmanuel J Candès and Terence Tao. **The power of convex relaxation: Near-optimal matrix completion**. *Information Theory, IEEE Transactions on*, **56**(5):2053–2080, 2010. 6, 29

[18] Emmanuel J Candes, Thomas Strohmer, and Vladislav Voroninski. **Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming**. *Communications on Pure and Applied Mathematics*, **66**(8):1241–1274, 2013. 6

[19] Emmanuel J Candes and Xiaodong Li. **Solving quadratic equations via PhaseLift when there are about as many equations as unknowns**. *Foundations of Computational Mathematics*, **14**(5):1017–1026, 2014. 6

[20] Emmanuel J Candes, Yonina C Eldar, Thomas Strohmer, and Vladislav Voroninski. **Phase retrieval via matrix completion**. *SIAM Review*, **57**(2):225–251, 2015. 6

[21] Jianxin Chen, Hillary Dawkins, Zhengfeng Ji, Nathaniel Johnston, David Kribs, Frederic Shultz, and Bei Zeng. **Uniqueness of quantum states compatible with given measurement results**. *Physical Review A*, **88**(1):012109, 2013. 6, 26

[22] Emmanuel J Candes, Xiaodong Li, and Mahdi Soltanolkotabi. **Phase retrieval via Wirtinger flow: Theory and algorithms**. *IEEE Transactions on Information Theory*, **61**(4):1985–2007, 2015. 6

[23] Praneeth Netrapalli, Prateek Jain, and Sujay Sanghavi. **Phase retrieval using alternating minimization**. In *Advances in Neural Information Processing Systems*, pages 2796–2804, 2013. 6

[24] Bernhard G Bodmann and Nathaniel Hammen. **Stable phase retrieval with low-redundancy frames**. *Advances in computational mathematics*, **41**(2):317–331, 2015. 6

[25] Bernhard G Bodmann and Nathaniel Hammen. **Algorithms and error bounds for noisy phase retrieval with low-redundancy frames**. *Applied and Computational Harmonic Analysis*, 2016. 6

[26] Stuart M Jefferies and Julian C Christou. **Restoration of astronomical images by iterative blind deconvolution**. *The Astrophysical Journal*, **415**:862, 1993. 7

[27] Lang Tong, Guanghan Xu, and Thomas Kailath. **Blind identification and equalization based on second-order statistics: A time domain approach**. *IEEE Transactions on information Theory*, **40**(2):340–349, 1994. 7

[28] Tony F Chan and Chiu-Kwong Wong. **Total variation blind deconvolution**. *IEEE transactions on Image Processing*, **7**(3):370–375, 1998. 7

[29] Ali Ahmed, Benjamin Recht, and Justin Romberg. **Blind deconvolution using convex programming**. *IEEE Transactions on Information Theory*, **60**(3):1711–1732, 2014. 7

[30] Xiaodong Li, Shuyang Ling, Thomas Strohmer, and Ke Wei. **Rapid, robust, and reliable blind deconvolution via nonconvex optimization**. *arXiv preprint arXiv:1606.04933*, 2016. 7

[31] Rémi Gribonval, Gilles Chardon, and Laurent Daudet. **Blind calibration for compressed sensing by convex optimization**. In *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2713–2716. IEEE, 2012. 7

[32] Shuyang Ling and Thomas Strohmer. **Self-calibration and biconvex compressive sensing**. *Inverse Problems*, **31**(11):115002, 2015. 7

[33] Sunav Choudhary and Urbashi Mitra. **Identifiability scaling laws in bilinear inverse problems**. preprint, arXiv:1402.2637, 2014. 7

BIBLIOGRAPHY

[34] Shobhit Choudhary and Urbashi Mitra. **Sparse blind deconvolution: What cannot be done**. In *IEEE Intl. Symp. Inform. Theory (ISIT)*, pages 3002–3006. IEEE, 2014. 7

[35] Y. Li, K. Lee, and Y. Bresler. **Identifiability in Blind Deconvolution With Subspace or Sparsity Constraints**. *IEEE Transactions on Information Theory*, **62**(7):4266–4275, July 2016. 7

[36] Yanjun Li, Kiryung Lee, and Yoram Bresler. **Identifiability in Blind Deconvolution under Minimal Assumptions**. preprint, arXiv:1507.01308, 2015. 7

[37] Yi-Kai Liu. **Universal low-rank matrix recovery from Pauli measurements**. In *Advances in Neural Information Processing Systems*, pages 1638–1646, 2011. 8, 12, 28, 29, 30

[38] Steven T Flammia, David Gross, Yi-Kai Liu, and Jens Eisert. **Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators**. *New Journal of Physics*, **14**(9):095022, 2012. 8, 12, 28, 29, 30, 31

[39] D Goyeneche, G Canas, S Etcheverry, ES Gómez, GB Xavier, G Lima, and A Delgado. **Five measurement bases determine pure quantum states on any dimension**. *Physical review letters*, **115**(9):090401, 2015. 8

[40] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010. 11

[41] Victor Guillemin and Alan Pollack. *Differential topology*, **370**. American Mathematical Soc., 2010. 11, 26, 27

[42] Frank W Warner. *Foundations of differentiable manifolds and Lie groups*, **94**. Springer, 1971. 11

[43] Michael M Wolf. **Quantum channels & operations: Guided tour**. *Lecture notes available at http://www-m5. ma. tum. de/foswiki/pub M*, **5**, 2012. 14

[44] Karl Kraus. *States, effects and operations*. Springer, 1983. 16

[45] Man-Duen Choi. **Completely positive linear maps on complex matrices**. *Linear Algebra and its Applications*, **10**(3):285 – 290, 1975. 16

[46] W. Forrest Stinespring. **Positive functions on C*-algebras**. *Proceedings of the American Mathematical Society*, **6**(2):211–216, 1955. 16

[47] K Vogel and H Risken. **Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase**. *Physical Review A*, **40**(5):2847, 1989. 19

[48] Zdenek Hradil. **Quantum-state estimation**. *Physical Review A*, **55**(3):R1561, 1997. 19

[49] Zdeněk Hradil, Jaroslav Řeháček, Jaromír Fiurášek, and Miroslav Ježek. **Maximum-likelihood methods in quantum mechanics**. In *Quantum state estimation*, pages 59–112. Springer, 2004. 19

[50] J Řeháček, Z Hradil, and M Ježek. **Iterative algorithm for reconstruction of entangled states**. *Physical Review A*, **63**(4):040303, 2001. 19

[51] K Banaszek, GM D'ariano, MGA Paris, and MF Sacchi. **Maximum-likelihood estimation of the density matrix**. *Physical Review A*, **61**(1):010304, 1999. 19

[52] Daniel FV James, Paul G Kwiat, William J Munro, and Andrew G White. **Measurement of qubits**. *Physical Review A*, **64**(5):052312, 2001. 19

[53] CF Roos, GPT Lancaster, M Riebe, H Häffner, W Hänsel, S Gulde, C Becher, J Eschner, F Schmidt-Kaler, and R Blatt. **Bell states of atoms with ultralong lifetimes and their tomographic state analysis**. *Physical review letters*, **92**(22):220402, 2004. 19

[54] Kevin J Resch, Philip Walther, and Anton Zeilinger. **Full characterization of a three-photon Greenberger-Horne-Zeilinger state using quantum state tomography**. *Physical review letters*, **94**(7):070402, 2005. 19

[55] S Filipp, P Maurer, PJ Leek, M Baur, R Bianchetti, JM Fink, M Göppl, L Steffen, JM Gambetta, A Blais, et al. **Two-qubit state tomography using a joint dispersive readout**. *Physical review letters*, **102**(20):200402, 2009. 19

[56] Jonathan P Home, David Hanneke, John D Jost, Jason M Amini, Dietrich Leibfried, and David J Wineland. **Complete methods set for scalable ion trap quantum information processing**. *Science*, **325**(5945):1227–1230, 2009. 19

[57] Julio T Barreiro, Markus Müller, Philipp Schindler, Daniel Nigg, Thomas Monz, Michael Chwalla, Markus Hennrich, Christian F Roos, Peter Zoller, and Rainer Blatt. **An open-system quantum simulator with trapped ions**. *Nature*, **470**(7335):486–491, 2011. 19

[58] Carl W Helstrom. *Quantum detection and estimation theory*, **123**. Academic press, 1976. 19

[59] KRW Jones. **Principles of quantum inference**. *Annals of Physics*, **207**(1):140–170, 1991. 19

[60] Ruediger Schack, Todd A Brun, and Carlton M Caves. **Quantum bayes rule**. *Physical Review A*, **64**(1):014305, 2001. 19

[61] Richard D Gill and Serge Massar. **State estimation for large ensembles**. *Physical Review A*, **61**(4):042312, 2000. 19

[62] Koenraad MR Audenaert and Stefan Scheel. **Quantum tomographic reconstruction with error bars: a Kalman filter approach**. *New Journal of Physics*, **11**(2):023028, 2009. 19

[63] Robin Blume-Kohout. **Optimal, reliable estimation of quantum states**. *New Journal of Physics*, **12**(4):043034, 2010. 19

[64] Robin Blume-Kohout. **Hedged maximum likelihood quantum state estimation**. *Physical review letters*, **105**(20):200504, 2010. 19

[65] Yong Siah Teo, Huangjun Zhu, Berthold-Georg Englert, Jaroslav Řeháček, and Zdeněk Hradil. **Quantum-state reconstruction by maximizing likelihood and entropy**. *Physical review letters*, **107**(2):020404, 2011. 19

[66] Matthias Christandl and Renato Renner. **Reliable quantum state tomography**. *Physical review letters*, **109**(12):120403, 2012. 19

[67] Robin Blume-Kohout. **Robust error bars for quantum tomography**. *arXiv preprint arXiv:1202.5270*, 2012. 19

[68] Jean-Pierre Amiet and Stefan Weigert. **Reconstructing the density matrix of a spin s through Stern-Gerlach measurements: II**. *Journal of Physics A: Mathematical and General*, **32**(25):L269, 1999. 20

[69] Steven T Flammia, Andrew Silberfarb, and Carlton M Caves. **Minimal informationally complete measurements for pure states**. *Foundations of Physics*, **35**(12):1985–2006, 2005. 20

[70] Morris W Hirsch. **Immersions of manifolds**. *Transactions of the American Mathematical Society*, **93**(2):242–276, 1959. 22

[71] John Willard Milnor and James D Stasheff. *Characteristic classes*, **93**. Princeton University Press Princeton, 1974. 23

[72] Allen Hatcher. **Vector bundles and K-theory**. *http://www. math. cornell. edu/~ hatcher*, 2003. 23

[73] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. **Tasks and premises in quantum state determination**. *Journal of Physics A: Mathematical and Theoretical*, **47**(7):075302, 2014. 26

[74] Ricardo Mañé. **On the dimension of the compact invariant sets of certain non-linear maps**. In *Dynamical Systems and Turbulence, Warwick 1980*, pages 230–242. Springer, 1981. 28

[75] Brian R Hunt and Vadim Yu Kaloshin. **Regularity of embeddings of infinite-dimensional fractal sets into finite-dimensional spaces**. *Nonlinearity*, **12**(5):1263, 1999. 28

[76] Christian Schwemmer, Géza Tóth, Alexander Niggebaum, Tobias Moroder, David Gross, Otfried Gühne, and Harald Weinfurter. **Experimental comparison of efficient tomography schemes for a six-qubit state**. *Physical review letters*, **113**(4):040503, 2014. 28

[77] Emmanuel J Candès and Benjamin Recht. **Exact matrix completion via convex optimization**. *Foundations of Computational mathematics*, **9**(6):717–772, 2009. 29

[78] Jos F Sturm. **Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones**. *Optimization methods and software*, **11**(1-4):625–653, 1999. 29

[79] Jian-Feng Cai, Emmanuel J Candès, and Zuowei Shen. **A singular value thresholding algorithm for matrix completion**. *SIAM Journal on Optimization*, **20**(4):1956–1982, 2010. 29

[80] Stephen R Becker, Emmanuel J Candès, and Michael C Grant. **Templates for convex cone problems with applications to sparse signal recovery**. *Mathematical programming computation*, **3**(3):165–218, 2011. 29

[81] Shiqian Ma, Donald Goldfarb, and Lifeng Chen. **Fixed point and Bregman iterative methods for matrix rank minimization**. *Mathematical Programming*, **128**(1-2):321–353, 2011. 29

[82] Balas Kausik Natarajan. **Sparse approximate solutions to linear systems**. *SIAM journal on computing*, **24**(2):227–234, 1995. 29

[83] Emmanuel J Candes and Yaniv Plan. **Tight oracle inequalities for low-rank matrix recovery from a minimal number of noisy random measurements**. *IEEE Transactions on Information Theory*, **57**(4):2342–2359, 2011. 30

[84] Jeongwan Haah, Aram W Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. **Sample-optimal tomography of quantum states**. *arXiv preprint arXiv:1508.01797*, 2015. 31

The Role of Topology in Quantum Tomography

M. Kech, P. Vrana and M. Wolf August 24, 2016

Quantum tomography is considered in the scenario where prior information constrains the set of relevant quantum states to a smooth submanifold of the state space. Starting from the topological approach taken in [1], a general framework is provided to lower bound the number of binary measurement settings needed to discriminate any two states of a given submanifold. Furthermore, the framework is applied to several concrete scenarios.

1 Stability and Smooth Embeddings

Let $POVM_{\mathcal{H}}^m$ be the set of POVMs on $\mathcal{H}$ with m outcomes. The set $POVM_{\mathcal{H}}^m$ is equipped with the topology induced by the metric $d(P,P') := \|D_P - D_{P'}\|_\infty$, $\forall P, P' \in POVM_{\mathcal{H}}^m$.

Definition 1 (Stability)**.** Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a subset. A POVM $P \in POVM_{\mathcal{H}}^m$ is called stably $\mathcal{R}$-complete iff there exists a neighbourhood $\mathcal{N} \subseteq POVM_{\mathcal{H}}^m$ of P such that the restricted map $D_{P'}|_{\mathcal{R}}$ is injective for all $P' \in \mathcal{N}$.

As the following theorem shows, if the subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ is a closed manifold this notion of stability is equivalent to the restricted measurement map being a smooth embedding. Consequently, under the premise of stability, non-embedding results for a manifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ yield lower bounds on the number of binary measurement settings needed to discriminate any two points of $\mathcal{P}$.

Theorem 1. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a closed manifold. A POVM $P \in POVM_{\mathcal{H}}^m$ is stably $\mathcal{P}$-complete iff $D_P|_{\mathcal{P}}$ is a smooth embedding.*

The following theorem shows that, when allowing for measurements on many copies of the unknown state, the minimal number of binary measurement settings needed to discriminate any two states of a closed manifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ is precisely the embedding dimension of $\mathcal{P}$. Let $\iota_k : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H}^{\otimes k})$, $\varrho \mapsto \varrho^{\otimes k}$.

Theorem 2. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a closed manifold. There exists a smooth embedding of $\mathcal{P}$ into Euclidean space of dimension m iff, for some $k \in \mathbb{N}$, there exists a stably $\iota_k(\mathcal{P})$-complete POVM $P \in POVM_{\mathcal{H}^{\otimes k}}^{m+1}$*

2 Application

For $n \in \mathbb{N}$, let $\alpha(n)$ be the number of ones in the binary expansion of n. Furthermore, for $n \in \mathbb{N}$ and $k \in \{1, \ldots, n\}$, let $\alpha_1(n) := \sum_{i=0}^{n-1} \alpha(i)$ and $\beta(n,k) := \alpha_1(n) - \alpha_1(k) - \alpha_1(n-k)$. Let $s = ((s_1, n_1), \ldots, (s_r, n_r)) \in (\mathbb{R} \times \mathbb{N})^r$ be such that $s_1 \geq 0$, $s_{i+1} \geq s_i$ for

all $i \in \{1, \ldots, r-1\}$, $\sum_{i=1}^{r} n_i s_i = 1$ and $\sum_{i=1}^{r} n_i = n$. Denote by $\mathcal{S}(s) \subseteq \mathcal{S}(\mathcal{H})$ the set of all quantum states with spectrum s. Then, $\mathcal{S}(s)$ is diffeomorphic to the complex flag manifold $U(n)/U(n_1) \times \ldots \times U(n_r)$ and Proposition 7 of [2] together with Theorem 1 yield the following result.

Theorem 3 (States of fixed spectrum)**.** *Let $m(s)$ be the smallest number such that there exists a stably $\mathcal{S}(s)$-complete POVM $P \in POVM_{\mathcal{H}}^{m(s)}$. Then, for all subsets $K \subseteq \{1, \ldots, r\}$ it holds that*

$$m(s) > 4k(n-k) - 2\beta(n,k) + 1$$

where $k := \sum_{i \in K} n_i$.

Let $\alpha \in \mathcal{H}_A \otimes \mathcal{H}_B$ with Schmidt rank k such that $\|\alpha\| = 1$. Let

$$\mathcal{S}_B(\alpha) := \{\beta\beta^* \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B) |\, \beta = (\mathbb{1} \otimes U)\alpha,\ U \in U(\mathcal{H}_B)\}$$

be the Bob unitary orbit of α. Furthermore, for $n, k \in \mathbb{N}$ with $n \geq k$ let

$$N(n,k) := \min\left\{ n-k < i \leq n : \binom{n}{i} \pmod 2 = 1 \right\},$$
$$\sigma(n,k) := 2 \cdot \max\left\{ 0 \leq i < N(n,k) : \binom{nk+i-1}{i} \pmod 2 = 1 \right\}.$$

Theorem 4 (Bob unitary orbit)**.** *Let $m(\alpha)$ be the smallest number such that there exists a stably $\mathcal{S}_B(\alpha)$-complete POVM $P \in POVM_{\mathcal{H}}^{m(\alpha)}$. Then, one has*

$$m(\alpha) > (2n-k)k + \sigma(n,k) + 1.$$

The set $\mathcal{S}_B(\alpha)$ is diffeomorphic to the complex projective Stiefel manifold $PW_{n,k} := \{[M] \in P(\mathbb{C}^{n \times k}) : M^*M = \mathbb{1}_k\}$ and the previous theorem is proven by computing the Stiefel-Whitney class of the tangent bundle of $PW_{n,k}$.

3 Legal statement

The project was assigned by Prof. Michael Wolf. I am the principal author of this article and I was significantly involved in all parts of this article.

References

[1] Teiko Heinosaari, Luca Mazzarella, and Michael M Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318(2):355–374, 2013.

[2] Markus Walgenbach. Lower bounds for the immersion dimension of homogeneous spaces. *Topology and its Applications*, 112(1):71–86, 2001.

IOP Publishing Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor. **48** (2015) 265303 (30pp) doi:10.1088/1751-8113/48/26/265303

The role of topology in quantum tomography

Michael Kech[1,3], Péter Vrana[2] and Michael M Wolf[1]

[1] Department of Mathematics, Technische Universität München, D-85748 Garching, Germany
[2] Department of Geometry, Budapest University of Technology and Economics, Egry József u. 1., 1111 Budapest, Hungary

E-mail: kech@ma.tum.de, vranap@math.bme.hu and wolf@ma.tum.de

Received 8 April 2015, revised 18 May 2015
Accepted for publication 18 May 2015
Published 12 June 2015

Abstract

We investigate quantum tomography in scenarios where prior information restricts the state space to a smooth manifold of lower dimensionality. By considering stability we provide a general framework that relates the topology of the manifold to the minimal number of binary measurement settings that is necessary to discriminate any two states on the manifold. We apply these findings to cases where the subset of states under consideration is given by states with bounded rank, fixed spectrum, given unitary symmetry or taken from a unitary orbit. For all these cases we provide both upper and lower bounds on the minimal number of binary measurement settings necessary to discriminate any two states of these subsets.

Keywords: quantum tomography, immersions, topology

(Some figures may appear in colour only in the online journal)

1. Introduction

The reconstruction of a quantum state from the outcome of an experiment, called quantum state tomography, is a task of fundamental importance in quantum information science. Already for small systems this task may be non-trivial, requiring many measurements and extensive postprocessing to reconstruct a state. With growing system size this complexity becomes exceedingly relevant [1].

There are at least three kinds of resources that can be considered in this context: (i) the number of measurement settings or, mathematically equivalent, the number of measurement

[3] Author to whom any correspondence should be addressed.

outcomes if a single generalized measurement is considered, (ii) the number of samples to be measured, i.e., the sampling complexity, which takes the statistics into account and (iii) the classical post-processing that is required to interpret the data. In this work we will focus on (i).

We are interested in cases where prior information is available that effectively restricts the state space to a submanifold of lower dimensionality. This information may concern the rank of the density operator, its spectrum, symmetry, energy, associated particle number or other properties and combinations thereof.

The question behind our analysis is: what is the minimal number of binary measurement settings that is required to uniquely identify the state under the assumption that it is taken from the given submanifold? Motivated by the results in [2] our aim is a better understanding of the relation between the minimal number of required measurement settings and the topology of the considered submanifold. Such a relation is most clear in low dimensional examples: suppose the submanifold forms a Klein bottle. Then, although it is two-dimensional, it requires at least four binary measurement settings to identify every point since, loosely speaking, in less than four dimensions the Klein bottle has no realization without self-intersections.

This topological reasoning was introduced in [2] and there applied successfully for instance to the case of pure state quantum tomography. The latter has been a topic of active research in quantum information theory [2–12], closely related to the problem of phase retrieval [13, 14].

On a Hilbert space of dimension d, the set of pure states is of dimension $2d - 2$, whereas the set of all states is of dimension $d^2 - 1$. Consequently, in order to uniquely identify an arbitrary state, one has to at least perform $d^2 - 1$ different binary measurements, whereas in the case of pure states one can hope that $\mathcal{O}(d)$ measurements suffice to uniquely identify a state. In [2] it was shown that to leading order $4d$ binary measurements are necessary and sufficient to identify pure states and the compressed sensing approach of [11, 12, 15] provides an algorithm based on $\mathcal{O}(\mathrm{d}r\,\log(d))$ binary measurements with which a $d \times d$ matrix of rank r can be reliably identified.

The approach we take in this paper extends the results of [2] and gives a general framework for the validity of the topological reasoning in quantum tomography. Thereby, we show that the approach is applicable in the presence of of statistical fluctuations, imprecise prior information or inaccuracies in the implementation of the measurement set-up. Moreover, we provide a detailed analysis of a variety of old and new examples of submanifolds.

Outline. We consider measurements as smooth maps from a smooth submanifold of states into Euclidean space. The methods we deploy to find bounds on the number of measurement outcomes necessary to identify a state of a given submanifold uniquely rely on the technical assumption that this smooth map is a smooth embedding.

In section 3 we give an operational meaning of the smooth embedding assumption and we determine the relation of quantum tomography to the embedding problem in differential topology.

First, in section 3.1, we justify the smooth embedding assumption by relating it to properties one would generally require of measurements. More precisely, we give two natural notions of stability and we show that these are in fact equivalent to the measurement being a smooth embedding. In the sense of these stability properties our approach is robust with respect to noise.

Secondly, in section 3.2, we generalize the measurement scheme by allowing for measurements on several copies of a state. We then show that any smooth embedding can be approximated by these generalized measurements. This proves that asking for the minimal number of measurement that is needed to identify all states of a given submanifold of states is equivalent to asking for the minimal dimension in which this manifold can be embedded.

Having justified our methods of finding bounds in section 3, we devote section 4 to applying this method in concrete scenarios. We obtain upper and lower bounds on the number of measurement outcomes necessary to identify states of certain interesting submanifolds. The lower bounds result from topological obstructions, whereas the upper bounds rely on the explicit construction of measurement schemes. The methods used in this section are very different from the the ones used in the first two sections and from this point of view section 4 can be read independently.

First, we investigate states of fixed spectrum and we relate these to states of bounded rank in section 4.1. More precisely, we present lower bounds on the number of measurements necessary to identify states of fixed spectrum and these lower bounds turn out to be very close to the upper bounds for states of bounded rank obtained in [2]. In this way we obtain good upper and lower bounds for both the states of fixed spectrum and the states with bounded rank.

In section 4.2, we obtain lower and upper bounds for states with a unitary symmetry and we use this to obtain both lower and upper bounds for states of fixed spectrum with a unitary symmetry in section 4.3.

Finally, in section 4.4, we obtain upper and lower bounds for states in a bipartite system that lie in the Bob-unitary orbit of a certain pure state, i.e. we consider all states that can be reached from a given pure state by acting with a unitary matrix that just effects Bob's subsystem. Physically, this scenario may correspond to an interferometry experiment. Note that if the initial state is maximally entangled, this orbit is the set of maximally entangled states which may be interesting in its own right. Identifying a maximally entangled state is equivalent to determining the unitary matrix that acted on Bob's subsystem. So this method can also be used for process-tomography of unitary time evolutions, complementing the results in [16, 17].

Proofs of technical results can be found in the appendix.

2. Preliminaries

Let $\mathcal{H}$ be a finite dimensional Hilbert space. We denote by $\mathcal{B}(\mathcal{H})$ the complex vector space of linear operators on $\mathcal{H}$. $H(\mathcal{H})$ denotes the real vector space of hermitian operators on $\mathcal{H}$ and $H(\mathcal{H})_0$ denotes the real vector space of traceless hermitian matrices, i.e. $H(\mathcal{H})_0 := \{h \in H(\mathcal{H}) : \mathrm{tr}(h) = 0\}$. Throughout we consider these spaces as inner product spaces equipping them with the Hilbert–Schmidt inner product. Furthermore, $\mathcal{S}(\mathcal{H})$ will denote the set of quantum states on $\mathcal{H}$, i.e. $\mathcal{S}(\mathcal{H}) := \{\rho \in H(\mathcal{H}) : \rho \geqslant 0, \mathrm{tr}(\rho) = 1\}$.

A positive operator valued measure (POVM) corresponds to a set of positive semidefinite operators $P := \{P_1, \ldots, P_m\}$ in $H(\mathcal{H})$ such that

$$\sum_{i=1}^{m} P_i = \mathbb{1}_{\mathcal{H}}.$$

An element of P is called an effect operator. We define the dimension of P by $\dim P = m - 1$. In quantum mechanics, POVMs are used to describe general measurements [18, 19].

There is an operator system[4] σ_P associated to each POVM P given by the complex linear span of the operators of P. For an operator system σ denote by $\sigma^{\mathbb{R}}$ the real vector space of

[4] An operator system $\sigma \subseteq \mathcal{B}(\mathcal{H})$ is a linear subspace such that $\mathbb{1}_{\mathcal{H}} \in \sigma$ and $\sigma^{\dagger} = \sigma$.

hermitian operators in σ, i.e. $\sigma^{\mathbb{R}} \coloneqq \{h \in \sigma : h^{\dagger} = h\}$[5]. In the following we assume the effect operators of a POVM P to be linearly independent over $\mathbb{C}$. Note that by this convention $\dim P = \dim \sigma_P - 1$. To each operator system σ one can associate the orthogonal projection from $H(\mathcal{H})$ to $\sigma^{\mathbb{R}} \subseteq H(\mathcal{H})$. Throughout we denote this associated projection by π_σ.

Definition 2.1. A POVM $P \coloneqq \{P_1, \ldots, P_m\}$ induces a linear map

$$h_P : H(\mathcal{H}) \to \mathbb{R}^m,$$
$$\rho \mapsto \big(\mathrm{tr}(P_1\rho), \ldots, \mathrm{tr}(P_m\rho)\big).$$

P is called $\mathcal{R}$-complete for a subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ if $h_P|_{\mathcal{R}}$ is injective and it is called $\mathcal{P}$-embedding for a smooth submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ if $h_P|_{\mathcal{P}}$ is a smooth embedding[6].

Recall that the question behind our analysis concerns the minimal m for which there is a $\mathcal{P}$-complete POVM for a given smooth submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ that characterized the available prior information. From the dimension $D \coloneqq \dim \mathcal{P}$ alone one obtains that $m \geqslant D$ is necessary and $m = 2D + 1$ is generally sufficient [2]. For better bounds, one has to invoke more of the (topological) structure of the manifold.

In the following all manifolds and submanifolds are assumed to be smooth. Throughout we regard both $\mathcal{S}(\mathcal{H})$ and submanifolds $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ with $\mathcal{H} \simeq \mathbb{C}^n$ as submanifolds of $H(\mathcal{H}) \simeq \mathbb{R}^{n^2}$ equipped with the subspace topology and the standard smooth structure. We often use this picture to identify the tangent space at a point $\rho \in \mathcal{P}$, $T_\rho\mathcal{P}$, with a linear subspace in $H(\mathcal{H})$, i.e. we think of tangent vectors $v \in T_\rho\mathcal{P}$ as hermitian operators. We assume submanifolds $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ to be closed and without boundary. In particular, this means that $\mathcal{P}$ is an embedded submanifold by the compactness of $\mathcal{S}(\mathcal{H})$, i.e. the inclusion is a homeomorphism onto its image.

3. Topological analysis of measurements

3.1. Stable measurements

Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a submanifold. In order for our methods for finding bounds on the dimension of $\mathcal{P}$-complete POVMs to apply, we need the technical requirement that these POVMs are $\mathcal{P}$-embeddings. In this section we justify this assumption. We develop two notions of stability for a $\mathcal{P}$-complete POVM and we show that these notions are equivalent to the POVM being a $\mathcal{P}$-embedding. These notions of stability are properties one would naturally require for $\mathcal{P}$-complete POVMs. Thus, under the premise of stability, $\mathcal{P}$-complete POVMs are $\mathcal{P}$-embeddings.

For a given POVM P the notions of $\mathcal{P}$-embedding and $\mathcal{P}$-completeness just depend on its associated operator system σ_P as the following proposition shows.

Proposition 3.1. *Let* P *be a POVM,* $\mathrm{h_P}$ *be the associated linear map,* $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ *be a submanifold and let* $\pi_P : H(\mathcal{H}) \to \sigma_P^{\mathbb{R}}$ *be the orthogonal projection on* $\sigma_P^{\mathbb{R}}$.

1. P *is* $\mathcal{P}$*-complete if and only if* $\pi_P|_{\mathcal{P}}$ *is injective.*

[5] Note that $\sigma^{\mathbb{R}}$ determines σ uniquely.

[6] A smooth mapping $\psi : M \to N$ is called a smooth embedding if $\mathrm{d}\psi_x$ is injective for all $x \in M$ and ψ is a homeomorphism onto its image.

2. P *is a* $\mathcal{P}$*-embedding if and only if* $\mathrm{h_P}$ *is* $\mathcal{P}$*-complete and* $d(\pi_P|_{\mathcal{P}})_\rho = \pi_P|_{T_\rho}$ *P is injective for each* $\rho \in \mathcal{P}$.

Proof. Since we equipped $H(\mathcal{H})$ with the Hilbert–Schmidt inner product, by the definition of h_P, we get $\sigma_P^{\mathbb{R}} = \mathrm{span}_{\mathbb{R}} P \subseteq \ker(h_P)^\perp$ and since rank $h_P = \dim \sigma_P^{\mathbb{R}}$, we get $\sigma_P^{\mathbb{R}} = \ker(h_P)^\perp$ by dimensional reasons. So $h_P = h_P \circ \pi_P$.

For the first statement, let P be $\mathcal{P}$-complete and h_P be the associated linear map. Since $h_P|_{\mathcal{P}}$ is injective and $h_P = h_P \circ \pi_P$, we get that $\pi_P|_{\mathcal{P}}$ is injective.

Conversely, let $\pi_P|_{\mathcal{P}}$ be injective. Then, since $h_P = h_P \circ \pi_P$, $h_P|_{\mathcal{P}}$ is injective because $\pi_P|_{\mathcal{P}}$ is injective and h_P is injective restricted to the image of π_P.

Noting that by linearity we have $\mathrm{d}(h_P|_{\mathcal{P}})_\rho = \mathrm{d}h_P|_{T_\rho \mathcal{P}} = h_P|_{T_\rho \mathcal{P}}$, the above reasoning also applies for the second statement. □

For a submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$, $\mathcal{P}$-completeness and being a $\mathcal{P}$-embedding are the only properties of a POVM we are interested in. Thus, by proposition 3.1, there is a natural equivalence relation on the set of POVMs, namely

$$P \sim P' \quad \Leftrightarrow \quad \sigma_P = \sigma_{P'}.$$

Since every n-dimensional operator system is generated by an $(n-1)$-dimensional POVM [2], the operator systems are precisely the equivalence classes.

Since the proofs we give are easier to formulate using operator system we often state our results in terms of operator systems and then transfer them to POVMs.

Let $\Sigma(n)$ be the set of n-dimensional operator systems. For a subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ we call $\sigma \in \Sigma(n)$ $\mathcal{R}$-complete if $\pi_\sigma|_{\mathcal{R}}$ is injective and for a submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ we call $\sigma \in \Sigma(n)$ a $\mathcal{P}$-embedding if $\pi_\sigma|_{\mathcal{P}}$ is a smooth embedding.

A metric on $\Sigma(n)$, which is natural for our purpose, can be defined in terms of any norm on the corresponding linear map π_σ. For an arbitrary linear map $L : H(\mathcal{H}) \to H(\mathcal{H})$ we consider

$$\|L\|_{op} = \sup_{B \in H(\mathcal{H}), \|B\| \leqslant 1} \|L(B)\|,$$

where $\|\cdot\|$ denotes the Hilbert–Schmidt norm. The sought metric is then given by $\mathrm{d}(\sigma, \sigma') = \|\pi_\sigma - \pi_{\sigma'}\|_{op}$. The following definition refers to the metric topology induced on $\Sigma(n)$.

Definition 3.2. (*Stability*). Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a subset. An $\mathcal{R}$-complete operator system $\sigma \in \Sigma(n)$ is called stably $\mathcal{R}$-complete if there exists a neighbourhood $N \subseteq \Sigma(n)$ of σ such that every $\sigma' \in N$ is an $\mathcal{R}$-complete operator system. A POVM P is called stably $\mathcal{R}$-complete if its associated operator system σ_P is $\mathcal{P}$-complete .

Remark. In the following we will see that closeness of POVMs is equivalent to closeness of the associated operators systems. Thus, this definition says that a stably $\mathcal{P}$-complete POVM P is robust against inaccuracy in its implementation in the sense that every close enough POVM is also $\mathcal{P}$-complete.

The intuition behind this definition is best envisioned by thinking of operator systems as planes in $H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$, see figure 1.

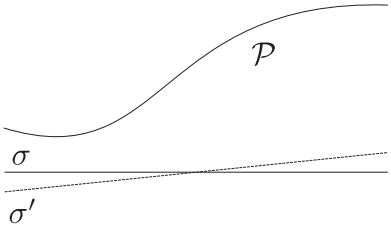

Figure 1. This figure shows a submanifold $\mathcal{P} \subseteq H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$ and two close operator systems $\sigma, \sigma' \subseteq H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$ that are $\mathcal{P}$-complete.

Now we are in a position to state one of the main results of this section.

Theorem 3.3. *(Stable measurements are embeddings). Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a closed submanifold and let $\sigma \in \Sigma(n)$ be $\mathcal{P}$-complete. Then σ is stably $\mathcal{P}$-complete if and only if it is a $\mathcal{P}$-embedding.*

Since the proof of this theorem is rather lengthy we relegated it to appendix A.1.

Theorem 3.3 is a statement about operator systems. In order to provide it with an operational meaning, we prove the corresponding stability result for POVMs in the following.

Corollary 3.4. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a closed submanifold and let $P := \{P_1, \ldots, P_m\}$ be a $\mathcal{P}$-complete POVM of dimension $m - 1$ with associated linear map $\mathrm{h_P}$. P is a $\mathcal{P}$-embedding if and only if there is an $\epsilon > 0$ such that every POVM Q with $\sup_{v \in H(\mathcal{H}), \|v\| \leqslant 1} \|(h_P - h_Q)v\| < \epsilon$ is $\mathcal{P}$-complete.*

Proof. Let $\mathcal{H} = \mathbb{C}^n$ and let π_P be the orthogonal projection associated to $P := \{P_1, \ldots, P_m\}$.

Let $\epsilon > 0$ such that every POVM Q with $\sup_{v \in H(\mathcal{H}), \|v\| \leqslant 1} \|(h_P - h_Q)v\|_2 < \epsilon$ is $\mathcal{P}$-complete. We show, that there is $\delta > 0$ such that for all $\sigma' \in \Sigma(m)$ with

$$\|\pi_P - \pi_{\sigma'}\|_{op} < \delta$$

there is a POVM $P' := \{P'_1, \ldots, P'_m\}$ with $\sigma_{P'} = \sigma'$ and $\sup_{v \in H(\mathcal{H}), \|v\| \leqslant 1} \|(h_P - h_{P'})v\|_2 < \epsilon$, hence $\pi_{\sigma'}$ is $\mathcal{P}$-complete by proposition 3.1.

For every $\eta > 0$, we can slightly deform P to a POVM $\tilde{P} := \{\tilde{P}_1, \ldots, \tilde{P}_m\}$ with full rank effect operators such that $\|P_i - \tilde{P}_i\| < \eta$ and $\sigma_P = \sigma_{\tilde{P}}$:let $\tilde{P}_i := \frac{\sqrt{n}}{\sqrt{n}+\eta}(P_i + \frac{\eta}{\sqrt{n}}\mathbb{1}_{\mathcal{H}})$ for $i = 1, \ldots, m$. Then, for $i = 1, \ldots, m$, $\|P_i - \tilde{P}_i\| = \eta\frac{\sqrt{n}}{\sqrt{n}+\eta} < \eta$. Note that we also ensured that the smallest eigenvalue of $\tilde{P}_i$ is bigger than $\eta/2$ for $i = 1, \ldots, m$ and η small enough.

For some $\sigma' \in \Sigma(m)$ with

$$\|\pi_P - \pi_{\sigma'}\|_{op} < \delta$$

let $P'_i := \pi_{\sigma'}(\tilde{P}_i)$, $i = 1, \ldots, m$. Then, for $i = 1, \ldots, m$

$$\|\tilde{P}_i - P'_i\| = \|\pi_P\left(\tilde{P}_i\right) - \pi_{\sigma'}\left(\tilde{P}_i\right)\| < \sqrt{n}\,\delta$$

and thus the P'_i are positive for $\sqrt{n}\,\delta < \eta/2$. Furthermore, $\sum_{i=1}^m P'_i = \pi_{\sigma'}(\sum_{i=1}^m \tilde{P}_i) = \pi_{\sigma'}(\mathbb{1}_{\mathcal{H}}) = \mathbb{1}_{\mathcal{H}}$. For small enough δ, the P'_i are linearly independent because the P_i are linearly

independent by assumption. Thus $\sigma' = \sigma_{P'}$ by dimensional reasoning. Finally

$$\begin{aligned}
&\|h_P - h_{P'}\|_{op}^2 \\
&\leqslant \sum_{i=1}^{m} \|P_i - P_i'\|^2 = \sum_{i=1}^{n} \|P_i - \tilde{P}_i + \tilde{P}_i - P_i'\|^2 \\
&\leqslant \sum_{i=1}^{m} \Big(\|P_i - \tilde{P}_i\| + \|\tilde{P}_i - P_i'\| \Big)^2 \\
&< m\Big(\eta^2 + n\delta^2\Big).
\end{aligned}$$

By choosing η and δ so small that $m(\eta^2 + n\delta^2) < \epsilon^2$, $h_{P'}$ is injective by assumption and thus σ' is injective by 3.1. Thus, σ_P is stably $\mathcal{P}$-complete and 3.3 concludes the proof of this direction.

Conversely, suppose σ is a $\mathcal{P}$-embedding. Corollary A.2 states, that there is an $\epsilon > 0$ such that every POVM Q with $\sup_{B\in H(\mathcal{H}),\|B\|\leqslant 1} \|h_P(B) - h_Q(B)\| < \epsilon$ is a $\mathcal{P}$-embedding and thus in particular $\mathcal{P}$-complete. □

However, the notion of stability for measurements developed so far may not be satisfactory yet since it just considers inaccuracy in the implementation of the measurement set-up. Noisiness of the outcome, resulting from e.g. dissipation or finite statistics, or noisiness of the input, originating from e.g. inaccurate prior information, are inevitable but not considered in the definition.

In the remainder of this section we show that also from this point of view, stably $\mathcal{P}$-complete is a operationally meaningful property.

The idea of the following lemma, which is the essential ingredient for the second theorem of this section, is to construct a neighbourhood for every point of submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ that can be approximated by the tangent space at that point. Let $\pi^T : \mathcal{P} \to \mathcal{B}(H(\mathcal{H}))$ be the mapping that associates to each point $\rho \in \mathcal{P}$ its orthogonal projection π_ρ^T to $T_\rho\mathcal{P} \subseteq H(\mathcal{H})$ and let π^N be the analogue mapping for the normal space, i.e. $\pi_\rho^N + \pi_\rho^T = \mathrm{id}_{H(\mathcal{H})}$ for all $\rho \in \mathcal{P}$. Furthermore, $B_x(\epsilon)$ denotes the open ball with center $x \in H(\mathcal{H})$ and radius $\epsilon > 0$, i.e. $B_x(\epsilon) \coloneqq \{y \in H(\mathcal{H}) : \|x - y\| < \epsilon\}$ and d denotes the metric induced by $\|\cdot\|$.

Lemma 3.5. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a submanifold. For every $\eta > 0$ there is an $\epsilon > 0$ such that for all $\rho \in \mathcal{P}$*

$$\rho' \in B_\epsilon(\rho) \bigcap \mathcal{P} \Rightarrow \|\pi_\rho^N(\rho' - \rho)\| < \eta \|\rho - \rho'\|.$$

Since the proof of this lemma in rather technical, it is relegated to appendix A.2.

The following theorem is the second main result of this section. It is formulated in terms of operator systems but again the result transfers to POVMs. Since the interpretation of the theorem may not be obvious let us first give some intuition and motivation: adding small perturbations to states of a submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ can be thought of as blowing up $\mathcal{P}$ to a small tubular neighbourhood $\mathcal{P}_\epsilon = \{\rho \in \mathcal{S}(\mathcal{H}) : d(\rho, \mathcal{P}) < \epsilon\}$. The dimension of $\mathcal{P}_\epsilon$ is then equal to the dimension of $H(\mathcal{H})$. Thus, one cannot expect $\mathcal{P}$-complete POVMs to stay injective when allowing for small errors. However, one can hope for being able to separate points in $\mathcal{P}_\epsilon$ that are sufficiently far away, in the sense that $\pi_P(\rho) \neq \pi_P(\rho')$ for $\|\rho - \rho'\| > C\epsilon$ with $C > 0$ a constant. For a given small enough ϵ such a C obviously exists however it is not immediate that C can be chosen independent of ϵ. The following theorem asserts that for ϵ

smaller than a certain fixed value, C is independent of ϵ. The existence of a C independent of ϵ means that the measurement can be made arbitrarily precise by reducing the errors.

Theorem 3.6. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a submanifold and let* P *be a POVM with associated orthogonal projection π_P.* P *is stably $\mathcal{P}$-complete if and only if there exists $\epsilon_0 > 0$ and $C > 2$ such that for all ϵ with $0 < \epsilon < \epsilon_0$*

$$\rho, \rho' \in \mathcal{P} \text{ with } \|\rho - \rho'\| > \epsilon C \;\Rightarrow\; \pi_P\big(B_\epsilon(\rho)\big) \bigcap \pi_P\Big(B_\epsilon\big(\rho'\big)\Big) = \varnothing.$$

Proof. Let P be stably $\mathcal{P}$-complete and thus a $\mathcal{P}$-embedding by theorem 3.3 and let $\rho \in \mathcal{P}$. Let $l \coloneqq \max_{\rho\in\mathcal{P}} \|\pi_P \circ \pi_\rho^T - \pi_\rho^T\|_{op}$ and let η as well as $\tilde{\epsilon}$ be as in lemma 3.5. Shrink ϵ_0 such that $C\epsilon_0 < \tilde{\epsilon}$.

Note that $l < 1$ because π_P is an immersion. Without the immersion property we could not assume $l < 1$ and in fact this is the essential idea of this proof[7].

Noting that $B = \{(\rho, \rho') \in \mathcal{P}^2 : \|\rho - \rho'\| \geqslant \epsilon_0 C\}$ is compact, $\kappa \coloneqq \min_{(\rho,\rho')\in B} \|\pi_P(\rho - \rho'\|$ is attained and thus $\kappa > 0$ by the injectivity of π_P. If necessary, shrink ϵ_0 such that $\epsilon_0 < \kappa/2$. Then, for $\rho' \in \mathcal{P} - (B_{C\epsilon_0}(\rho) \cap \mathcal{P})$ the claim holds because $\|\pi_P(\rho - \rho')\| \geqslant \kappa > 2\epsilon_0$ and $\pi_P(B_\epsilon(\rho)) = B_\epsilon(\pi_P(\rho))$.

Finally, let $\rho' \in B_{C\epsilon_0}(\rho) \cap \mathcal{P}$ and $\|\rho - \rho'\| > C\epsilon$, $0 < \epsilon < \epsilon_0$. Then

$$\begin{aligned}
\|\pi_P(\rho - \rho')\| &\geqslant \|\pi_P\Big(\pi_\rho^T(\rho - \rho')\Big)\| - \|\pi_P\Big(\pi_\rho^N(\rho - \rho')\Big)\| \\
&\geqslant \|\pi_P\Big(\pi_\rho^T(\rho - \rho')\Big) - \pi_\rho^T(\rho - \rho') + \pi_\rho^T(\rho - \rho')\| - \eta\,\|\rho - \rho'\| \\
&\geqslant \|\pi_\rho^T(\rho - \rho')\| - \|\pi_P\Big(\pi_\rho^T(\rho - \rho')\Big) - \pi_\rho^T(\rho - \rho')\| - \eta\,\|\rho - \rho'\| \\
&> \|\rho - \rho'\|\left(\sqrt{1 - \eta^2} - l - \eta\right) > \epsilon C\left(\sqrt{1 - \eta^2} - l - \eta\right),
\end{aligned}$$

where we used the fact that, for $0 \leqslant l < 1$, we can choose η small enough such that $\left(\sqrt{1 - \eta^2} - l - \eta\right) > 0$. Furthermore, we can choose $C > 0$ such that $C\left(\sqrt{1 - \eta^2} - l - \eta\right) > 2$. Since $\pi_P(B_\epsilon(\rho)) = B_\epsilon(\pi_P(\rho))$, this proves the statement.

For the converse, let $\rho, \rho' \in \mathcal{P}$ and $\rho \neq \rho'$. Choosing $\epsilon = \min\{\epsilon_0, \|\rho - \rho'\|/(2C)\}$, we find $\pi_P(B_\epsilon(\rho)) \cap \pi_P(B_\epsilon(\rho')) = \varnothing$ and thus $\pi_P(\rho) \neq \pi_P(\rho')$.

Finally, assume $\pi_P|_{\mathcal{P}}$ is not an immersion at some $\rho \in \mathcal{P}$. Let $\gamma : (-1, 1) \to \mathcal{P} \subseteq H(\mathcal{H})$ be a smooth curve with $\gamma(0) = \rho$ and $\frac{\mathrm{d}}{\mathrm{d}t}\gamma(0) = v \in \ker \pi_P$. Let $C > 0$ as in the theorem, then

$$2/C \leqslant \lim_{t\to 0} \frac{\|\pi_P(\gamma(t) - \rho)\|}{\|\gamma(t) - \rho\|} \leqslant \lim_{t\to 0} \frac{\|\pi_P(\gamma(t) - \rho)\|}{t/2} = 2\,\|\pi_P(v)\| = 0,$$

a contradiction. Here we assumed $\|\gamma(t) - \rho\| > t/2$ which is clearly true for t small enough by lemma 3.5. □

Remark. Note that it is essentially the constant l that determines C. For small l, i.e. in the case where the tangent spaces are not steep with respect to σ_P, we can ensure that C is close to

[7] The bigger l is, the steeper the tangent spaces can be with respect to the operator system σ_P. By the previous lemma we saw that small neighbourhoods around a point $\rho \in \mathcal{P}$ can be approximated by the tangent space at that point. We can ensure that these approximations are so good that the fluctuations around the steepest tangent space have no component orthogonal to σ_P and in this sense we can locally think of $\mathcal{P}$ as a plane.

2 (if we make ϵ_0 small enough). On the other hand if l is close to one C has to be big and in this sense l is a measure for the stability of the POVM P.

ϵ_0 is mainly determined by the constant κ, which is more of 'global' nature. Loosely speaking it is a measure for how bad $\mathcal{P}$ wiggles around in $H(\mathcal{H})$.

It is worth noting, that if π_P fails to be an immersion, $C \to \infty$ for $\epsilon \to 0$ and from this point of view, stably $\mathcal{P}$-complete measurements are the ones that can be made arbitrarily precise.

This theorem transfers to the corresponding theorem for POVMs as the following corollary shows.

Corollary 3.7. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a submanifold and let* P *be a POVM with associated linear map* $\mathrm{h_P}$. P *is a smooth embedding if and only if there exists $\epsilon_0 > 0$ and $C > 2$ such that for all* ϵ *with* $0 < \epsilon < \epsilon_0$

$$\rho, \rho' \in \mathcal{P} \text{ with } \|\rho - \rho'\| > \epsilon C \;\Rightarrow\; h_P\big(B_\epsilon(\rho)\big) \bigcap h_P\big(B_\epsilon(\rho')\big) = \varnothing.$$

Proof. Let π_P be the orthogonal projection associated to P. Let $\lambda := \min_{v \in \mathrm{supp}\, \pi_P, \|v\|=1} \|h_P(v)\|$ and observe that $\lambda > 0$ since h_P is injective on the support of π_P. Thus $\|h_P(\rho - \rho')\| = \|h_P \circ \pi_P(\rho - \rho')\| > \lambda \|\pi_P(\rho - \rho')\|$. Then, the proposition holds for h_P by replacing C with C/λ. □

Finally, this result also incorporates robustness against noisiness of the outcome as the following corollary shows.

Corollary 3.8. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a submanifold and let* P *be a stably $\mathcal{P}$-complete POVM with associated linear map* $\mathrm{h_P}$. *There exists $\epsilon_0 > 0$ and $C > 2$ such that for all* ϵ *with* $0 < \epsilon < \epsilon_0$

$$\mathcal{P} \bigcap h_P^{-1}\big(B_{2\epsilon}\big(h_P(\rho)\big)\big) \subseteq B_{C\epsilon}(\rho) \text{ for all } \rho \in \mathcal{P}.$$

Proof. Let C, ϵ_0 be as in corollary 3.7. Let $\rho \in \mathcal{P}$ and $\rho' \in h_P^{-1}(B_{2\epsilon}(h_P(\rho)))$ with $\|\rho - \rho'\| > C\epsilon$. Then, $2\epsilon < \|h_P(\rho) - h_P(\rho')\| < 2\epsilon$, a contradiction. □

3.2. Generalized measurements and smooth embeddings

Linear measurements are clearly not sufficient to realize all smooth embeddings. More precisely, if there is a smooth embedding $\phi : \mathcal{P} \subseteq \mathcal{S}(\mathcal{H}) \to \mathbb{R}^m$, then there need not be an m-dimensional POVM that is a $\mathcal{P}$-embedding. For example the set $N := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1, x \geqslant -0.5\}$ can clearly be embedded in $\mathbb{R}^1$, but an injective orthogonal projection has to have rank two. However, the embedding cannot get arbitrarily bad because from Whitney's embedding theorem we know that there is a $\mathcal{P}$-embedding in Euclidean space of twice the dimension of $\mathcal{P}$.

In this section we generalize our approach to measurements of the type

$$\mathrm{tr}\left(\rho^{\otimes n} P_i\right)$$

and we show that these measurements can approximate any smooth embedding. This means that if there exists a smooth embedding $\psi : \mathcal{P} \subseteq \mathcal{S}(\mathcal{H}) \to \mathbb{R}^m$, then there is POVM of dimension m that is a $\mathcal{P}$-embedding. Thus, the problem described in the beginning of this section can be circumvented by this generalized measurement scheme.

Let us fix some notation.

Definition 3.9. A measurement $P \coloneqq \{P_1, \ldots, P_m\}$ on k copies is a POVM on $H(\mathcal{H})^{\otimes k}$. P induces a linear map

$$h_P : H(\mathcal{H})^{\otimes k} \to \mathbb{R}^m,$$
$$\rho \mapsto \left(\mathrm{tr}\left(P_1\rho^{\otimes k}\right), \ldots, \mathrm{tr}\left(P_m\rho^{\otimes k}\right)\right).$$

Let $i : H(\mathcal{H}) \to H(\mathcal{H})^{\otimes k}$, $\rho \mapsto \rho^{\otimes k}$. P is called $\mathcal{R}$-complete for a subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ if $h_P \circ i\,|_{\mathcal{R}} = h_P\,|_{i(\mathcal{R})}$ is injective and it is called a $\mathcal{P}$-embedding for a submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ if $h_P\,|_{i(\mathcal{P})}$ is a smooth embedding.

The following proposition makes the connection to the theory developed in the last section.

Proposition 3.10. *The mapping $i : H(\mathcal{H}) \to H(\mathcal{H})^{\otimes k}$, $\rho \mapsto \rho^{\otimes k}$ is smooth. Furthermore, for a smooth closed submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$, $i\,|_{\mathcal{P}}$ is a smooth embedding.*

The proof of this proposition is relegated to appendix A.3.

Remark. Let $\Sigma(n, k)$ be the set of n-dimensional operator systems on $\mathcal{B}(\mathcal{H})^{\otimes k}$. Each n-dimensional measurement on k copies P generates an operator system $\sigma_P = \mathrm{span}\,\{P_i\}_{P_i \in P} \in \Sigma(n, k)$. If $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ is a closed submanifold, $i(\mathcal{P}) \subseteq \mathcal{S}(\mathcal{H}^{\otimes k}) = \mathcal{S}(\mathcal{H})^{\otimes k}$ is a closed submanifold by the previous proposition. So the ideas and results of the last section can be naturally applied to measurements on k copies. In particular for a submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ the notions of $\mathcal{P}$-embedding and $\mathcal{P}$-complete naturally apply to the equivalence classes $\sigma \in \Sigma(n, k)$ of measurements on k copies ($P \sim P' \Leftrightarrow \sigma_P = \sigma_{P'}$).

Theorem 3.11. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a closed submanifold and let $\sigma \in \Sigma(n, k)$ be $\mathcal{P}$-complete. Then σ is stably $\mathcal{P}$-complete if and only if it is a $\mathcal{P}$-embedding.*

Proof. By the previous remark $i(\mathcal{P}) \subseteq \mathcal{S}(\mathcal{H})^{\otimes k}$ is a closed submanifold. Then the claim follows by applying 3.3 to $i(\mathcal{P})$ and σ. □

Choosing an othonormal basis $\{\sigma_i\}_{i \in \{1,\ldots,d^2\}}$ of $H(\mathcal{H})$ with $\sigma_1 = \mathbb{1}_{\mathcal{H}}$ gives an identification $H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$. Under this identification we can think of elements in $H(\mathcal{H})^{\otimes k}$ as elements in $P^k(\mathbb{R}^{d^2})$, the vector space of polynomial functions of degree k on $H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$ [8].

[8] Note that by viewing $H(\mathcal{H})$ as a smooth manifold this corresponds to choosing a particular coordinate system $(x_1, \ldots, x_{d^2})$.

More precisely, let $\mathrm{Sym}(H(\mathcal{H}), k) \subseteq H(\mathcal{H})^{\otimes k}$ be the vector space of symmetric elements of degree k in $H(\mathcal{H})^{\otimes k}$. Then, use the identification $H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$ to define a linear map

$$\phi : \mathrm{Sym}(H(\mathcal{H}), k) \to P^k\left(\mathbb{R}^{d^2}\right) \tag{1}$$

by the relation

$$\phi(\eta)(x) = \mathrm{tr}\left(\eta\left(\sum_{i=1}^{n^2} x_i \sigma_i\right)^{\otimes n}\right),$$

where $\eta \in \mathrm{Sym}(H(\mathcal{H}), k)$ and $x \in \mathbb{R}^{d^2}$.

Lemma 3.12. *The mapping* ϕ *is an isomorphism.*

Proof. Let $d = \dim H(\mathcal{H})$. Note that

$$\dim \mathrm{Sym}\,(H(\mathcal{H}), k) = \binom{n+k-1}{k} = \dim P^k\left(\mathbb{R}^{d^2}\right).$$

Then, by linearity of ϕ, it is enough to check that ϕ is surjective. Under the identification $H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$, a basis of $P^k(\mathbb{R}^{d^2})$ is given by polynomials of the form $x_{i_1} \ldots x_{i_k}$, $i_j \in \{1, \ldots, d\}$, $i_1 \leqslant \cdots \leqslant i_k$. For each such polynomial $p = x_{i_1} \ldots x_{i_k}$ there is a $\eta \in \mathrm{Sym}\,(H(\mathcal{H}), k)$ such that $\phi(\eta)(x) = p$, namely $\eta = \sigma_{i_1} \cdot \ldots \cdot \sigma_{i_k}$, where $\cdot$ denotes the symmetric product. □

Remark. Note that every $\rho \in \mathcal{S}(\mathcal{H})$ decomposes as $\rho = \mathbb{1}_{\mathcal{H}} + \sum_{i=2}^{d^2} \sigma_i$ and thus $x_1 = 1$ on $\mathcal{S}(\mathcal{H})$. From this point of view $P^k(\mathbb{R}^{d^2})$ corresponds to $P^{\leqslant k}(\mathbb{R}^{d^2-1})$, the set of polynomials of degree $d \leqslant k$ in $x_2, \ldots, x_{d^2}$.

The following lemma is the crucial ingredient of the main theorem of this section. Let $\mathbb{1}_{\mathcal{H}} + H(\mathcal{H})_0 := \{\mathbb{1}_{\mathcal{H}} + h : h \in H(\mathcal{H})_0\}$.

Lemma 3.13. *Let* $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H}) \subseteq \mathbb{1}_{\mathcal{H}} + H(\mathcal{H})_0 \simeq \mathbb{R}^{n\times n-1}$ *be a closed submanifold and* $\psi : \mathcal{P} \to \mathbb{R}^m$ *be a smooth embedding. Then, there is a* $k \in \mathbb{N}$ *and a map* $\tilde{\psi}' = (p_1, \ldots, p_m)$, $p_i \in P^{\leqslant k}(\mathbb{R}^{n\times n-1})$, *such that* $\psi' = \tilde{\psi}'|_{\mathcal{P}}$ *is a smooth embedding.*

The proof of this lemma can be found in appendix A.4.

Theorem 3.14. *Let* $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ *be a closed submanifold. There is a smooth embedding of* $\mathcal{P}$ *in* $\mathbb{R}^m$ *if and only if, for some* $k \in \mathbb{N}$, *there exists a stably* $\mathcal{P}$*-complete* m*-dimensional measurement on* k *copies.*

Proof. 3.11 gives one direction. For the other direction, let $\psi : \mathcal{P} \to \mathbb{R}^m$ be a smooth embedding. Then, by 3.13, there is a smooth embedding $\psi' = (p_1, \ldots, p_m)|_{\mathcal{P}}$, $p_i \in P^{\leqslant k}(\mathbb{R}^{n\times n-1})$. $\sigma = \mathrm{span}_{\mathbb{R}}\{\mathbb{1}_{\mathcal{H}}, \phi^{-1}(p_1), \ldots, \phi^{-1}(p_m)\}$ (ϕ form 3.12) is clearly an operator system

whose dimension is less or equal to $m+1$. σ is a $\mathcal{P}$-embedding because $\psi'|_{\mathcal{P}}$ is an embedding and thus stably $\mathcal{P}$-complete by 3.11. □

Thus, under the premise of stability, asking for the minimal dimension of a $\mathcal{P}$-complete POVM is equivalent to the related problem in differential topology of finding the smallest m such that $\mathcal{P}$ can be smoothly embedded in $\mathbb{R}^m$.

4. Upper and lower bounds for concrete submanifolds

In this section we obtain lower as well as upper bounds on the dimension of complete and stable POVMs on some interesting submanifolds of states. The procedure is to first relate the submanifolds to well-known homogeneous spaces and then to obtain or use existing non-immersion results for these. Upper bounds are obtained by directly constructing POVMs.

First, we give bounds for the set of states with fixed spectrum. Thereby we also obtain bounds for the closely related set of states with bounded rank.

Then, we give a brief analysis of states with an underlying unitary symmetry which is needed in the next section, where we generalize the previous results to states of fixed spectrum with an underlying symmetry.

Finally, we obtain bounds for the set of pure states of bipartite systems, obtained from the action of the unitary group of the second system on some fixed pure state.

In the following let $\mathcal{H}=\mathbb{C}^n$.

4.1. States of fixed spectrum and states of bounded rank

First, we consider the set of states in $\mathcal{S}(\mathbb{C}^n)$ with fixed spectrum $s=(s_1,\ldots,s_n)$[9] and we denote by $D_s:=\mathrm{diag}(s_1,\ldots,s_n)$ the diagonal matrix with entries from s.

The set of all states with spectrum s, $\mathcal{S}(\mathbb{C}^n)_s$, is the orbit of D_s with respect to the action G of $U(n)$ on $\mathcal{S}(\mathbb{C}^n)$ by conjugation, i.e.

$$\mathcal{S}_s^n := \left\{ UD_sU^\dagger : \ U\in U(n)\right\}.$$

The isotropy group of ρ under this action is $U(n_1)\times\cdots\times U(n_k)$, where n_i is the multiplicity of the ith biggest eigenvalue. Note that $\sum_{j=1}^k n_j=n$. By theorem 3.62 of [20], factoring the orbit map over this isotropy group induces a diffeomorphism

$$U(n)/U\left(n_1\right)\times\cdots\times U(n_k)\simeq \mathcal{S}\left(\mathbb{C}^n\right)_s.$$

Thus, $\mathcal{S}_s^n$ can be identified with a complex flag manifold.

In [21], Walgenbach obtains lower bounds for the immersion dimension of complex flag manifolds. To present his result, we first introduce some notation.

Definition 4.1. Let $n\in\mathbb{N}$, $k\in\{0,1,\ldots,n\}$.

$$\begin{aligned}
&\alpha(n) := \text{number of ones in the binary expansion of } n,\\
&\alpha_1(n) := \sum_{i=0}^{n-1}\alpha(i),\\
&\beta(n,k) := \alpha_1(n)-\alpha_1(k)-\alpha_1(n-k).
\end{aligned}$$

Let $\{n_1,\ldots,n_k\}$ be a partition of n. Let K be some subset of $\{1,\ldots,k\}$ and set $m=\sum_{i\in K} n_i$.

[9] By spectrum we mean the set of eigenvalues order increasingly together with their multiplicities.

Proposition 4.2. *[21] The complex flag manifold* $U(n)/U(n_1) \times \cdots \times U(n_k)$ *cannot be immersed in Euclidean space of dimension* $4m(n-m) - 2\beta(n, m) - 1$ *and it cannot be embedded in Euclidean space of dimension* $4k(n-m) - 2\beta(n, m)$.

Next, we want to obtain upper bounds on the dimension of stably $\mathcal{S}_s^n$-complete POVMs. Let σ be the function that associates to each $h \in H(\mathbb{C}^n)$ its spectrum. For $A \subseteq H(\mathbb{C}^n)$, let $\mathrm{Spec}(A) \coloneqq \{D_s : s = \sigma(M), M \in A\}$ and let $G(A) \coloneqq \{UMU^\dagger : U \in U(n), M \in A\}$.

Lemma 4.3. $\Delta\mathcal{S}_s^n = G\big(\mathrm{Spec}(\Delta\mathcal{S}_s^n)\big)$ *and* $T\mathcal{S}_s^n = G\Big(\mathrm{Spec}(T_{D_s}\mathcal{S}_s^n)\Big)$ *as sets. Furthermore, let* r *be the biggest multiplicity of an eigenvalue in* s, *then* $\mathrm{rank}(M) < 2(n-r) + 1$ *for* $M \in \Delta\mathcal{S}_s^n \cup T\mathcal{S}_s^n$.

Proof. The first claim is essentially true by definition. For the second claim, let us compute the tangent space at M_s. Let $h \in H(\mathbb{C}^n)$ and consider the curve $\gamma : t \mapsto \mathrm{e}^{\mathrm{i}ht} D_s \mathrm{e}^{-\mathrm{i}ht}$. The derivative at $t = 0$ of this curve is then an element of $T_{D_s}S_s^n$ and we find

$$\frac{\mathrm{d}}{\mathrm{d}t}\gamma\,|_{t=0} = \frac{\mathrm{d}}{\mathrm{d}t}\,|_{t=0}\ \mathrm{e}^{\mathrm{i}ht} D_s \mathrm{e}^{-\mathrm{i}ht}\,|_{t=0} = \mathrm{i}\big[h, D_s\big].$$

In the canonical basis, these elements are of the form

$$\begin{pmatrix} 0 & \mathrm{i}A & \mathrm{i}B & \dots \\ \mathrm{i}A^\dagger & 0 & \mathrm{i}C & \\ \mathrm{i}B^\dagger & \mathrm{i}C^\dagger & 0 & \\ \vdots & & & \ddots \end{pmatrix}.$$

Thus, by dimensional reasons, all elements of $T_{D_s}S_s^n$ are of this form. Furthermore for $U \in U(n)$, observe that

$$U\big[h, D_s\big]U^\dagger = \Big[UhU^\dagger, UD_sU^\dagger\Big]$$

and thus

$$\begin{aligned} c_U : T_{D_s}S_s^n &\to T_{UD_sU^\dagger}S_s^n \\ v &\mapsto UvU^\dagger \end{aligned}$$

is an isomorphism. This proves the second claim. To prove the last claim, observe that for $U, V \in U(n)$

$$UD_sU^\dagger - VD_sV^\dagger = U\big(D_s - \lambda\mathbb{1}\big)U^\dagger - V\big(D_s - \lambda\mathbb{1}\big)V^\dagger$$

and similarly

$$\big[h, D_s\big] = \big[h, D_s\big] - [h, \lambda\mathbb{1}] = \big[h, D_s - \lambda\mathbb{1}\big].$$

Choosing λ to be the eigenvalue in s with the biggest multiplicity r, the expressions above are differences of rank $n - r$ matrices and thus maximally of rank $2(n-r)$. □

Remark. It is immediate that a POVM P, that is injective on the set of hermitian operators with rank smaller than r, $\mathcal{P}_r$, is an $\mathcal{S}_s^n$-embedding. This is because $\Delta\mathcal{P}_r = \mathcal{P}_{2r}$ and thus $\Delta\mathcal{S}_s^n \cup T\mathcal{S}_s^n = \mathcal{P}_{2r} = \Delta\mathcal{P}_r$ by 4.3.

As a consequence, the POVM constructed in [2] for states of bounded rank is also a S_s^n-embedding and we obtain the following upper bounds.

Proposition 4.4. *Let* m *be the biggest multiplicity of an eigenvalue in the spectrum* s *and let* $r := n - m$. *Then, there is a POVM* P *of dimension* $4r(n-r) - 1$ *that is a* S_s^n*-embedding.*

Remark. Note that for $r = n/2$ the dimension of the POVM is $4\, n/2(n - n/2) - 1 = n^2 - 1$. Thus, it is the trivial POVM that can identify all states and hence we also get a S_s^n-embedding for $r > n/2$.

The construction of the POVM is based on [22]. The idea is to use a totally non-singular matrix, like e.g. the Vandermonde-matrix, to construct a linear subspace of $M(\mathbb{C}, n)$ that just contains matrices of rank bigger than $2r$.

As presented in the table 1, these results are rather close to the lower bounds of [21]. Thus, the POVM of [2] gives good upper bounds on S_s^n and in addition we have indirectly obtained good lower bounds on the dimension of a POVM that is complete with respect to the states of bounded rank.

4.2. States with unitary symmetry

Next, we shortly discuss subsets of states invariant under some unitary subgroup.

More precisely, we analyze the structure of the fix point sets of the action by conjugation G_H of some subgroup $H \subseteq U(n)$, i.e.

$$\mathcal{S}\left(\mathbb{C}^n\right)_H := \left\{\rho \in \mathcal{S}\left(\mathbb{C}^n\right) :\ U\rho U^\dagger = \rho,\ \forall\, U \in H\right\}.$$

Consider the sets $\mathcal{B}(\mathbb{C}^n)_H := \{B \in \mathcal{B}(\mathbb{C}^n) :\ UBU^\dagger = B,\ \forall\, U \in H\}$. $\mathcal{B}(\mathbb{C}^n)_H$ is a C^* algebra, since it is certainly a vector space and closed under the *-involution by the unitarity of H and thus the structure theorem [23] yields that $\mathcal{B}(\mathbb{C}^n)_H$ is unitarily equivalent to $\bigoplus_{i=1}^k M(n_i, \mathbb{C}) \otimes \mathbb{1}_{m_i}$.

Observe that the linear isomorphism

$$\begin{aligned} \iota\colon \mathcal{S}\left(\bigoplus_{i=1}^k M\left(n_i, \mathbb{C}\right)\right) &\to \bigoplus_{i=1}^k M\left(n_i, \mathbb{C}\right) \otimes \mathbb{1}_{m_i} \\ (\rho_1, \ldots, \rho_k) &\mapsto \left(\frac{1}{m_1}\rho_1 \otimes \mathbb{1}_{m_i}, \ldots, \frac{1}{m_k}\rho_k \otimes \mathbb{1}_{m_k}\right). \end{aligned} \tag{2}$$

descends to a diffeomorphism on states. Form this we immediately get the following proposition.

Proposition 4.5. *There is a POVM* P *with* $\dim P = \dim \mathcal{S}(\mathbb{C}^n)_H$ *that is stably* $\mathcal{S}(\mathbb{C}^n)_H$*-complete.*

4.3. Unitarily invariant states of fixed spectrum

Now, given some unitary subgroup $H \subseteq U(n)$, we want to identify G_H-invariant (cf 4.2) states of fixed spectrum s[10], i.e.

[10] Here s has to be compatible with the decomposition illustrated in section 4.2.

Table 1. Dimension/lower bounds on immersion dimension [21]; upper bound on embedding dimension 4.4 for $U(l+k)/U(l) \times U(1)^k$.

l\k	2	3	4
5	22/34;39		
6	26/40;47		
7	30/50;55	48/76;83	
8	34/60;63	54/90;95	
9	38/66;71	60/98;107	84/134;143
10	42/72;79	66/110;119	92/148;159

Table 2. Lower bounds on immersions of $W_{n,1} \simeq P\mathbb{C}^n$ for $n = 2, \ldots, 17$. In the first row the result is obtained from the dual Stiefel–Whitney classes in the second row the results of [26] are presented.

2	6	6	14	14	14	14	30	30	30	30	30	30	30	62
2	6	8	14	16	21	22	30	32	37	38	45	46	52	52	62

Table 3. Lower bounds on immersion dimension of $PW_{n,r}$ obtained from dual Stiefel–Whitney classes 4.8.

n\r	2	3	4	5	6	7	8	9	10	11	12	13
2	2	3										
3	6	7	8									
4	6	11	14	15								
5	14	19	22	23	24							
6	14	27	30	31	34	35						
7	14	27	38	39	46	47	48					
8	14	27	38	47	54	59	62	63				
9	30	43	54	63	70	75	78	79	80			
10	30	51	54	63	86	91	94	95	98	99		
11	30	55	72	79	86	107	110	111	118	119	120	
12	30	59	78	79	102	107	126	127	134	139	142	143

$$\mathcal{S}\left(\mathbb{C}^n\right)_{H,s} := \left\{ \rho \in \mathcal{S}\left(\mathbb{C}^n\right) : \ U\rho U^\dagger = \rho, \forall\, U \in H, \operatorname{spec}(\rho) = s \right\}.$$

Via the map ι defined in (2), there is natural action of $U_{n_1} \times \cdots \times U_{n_k}$ on $B(\mathbb{C}^n)_H$ coming from its action on $\bigoplus_{i=1}^k M(n_i, \mathbb{C})$. $\mathcal{S}(\mathbb{C}^n)_H$ is then the orbit of this action on the set

$$\mathcal{D} := \left\{ \left(D_{M_1}, \ldots, D_{M_k}\right) : \left[\left(M_1\right)^{c_1} \bigcup \cdots \bigcup \left(M_k\right)^{c_k} \right] = s \right\}.$$

Here M_i is a multiset of order n_i and $(M_i)^{c_i}$ is the union of c_i copies of M_i. By the same argument as in the previous section the orbit of some $\rho \in \mathcal{D}$ under G_H is diffeomorphic to a product of complex flag manifolds $\prod_{i=1}^k U(n_i)/\prod_{j=1}^{k_j} U(n_j^i)$. Since $\mathcal{D}$ is clearly finite, $\mathcal{S}(\mathbb{C}^n)_{H,s}$ is a disjoint union of products of complex flag manifolds. Thus, it is enough to look at one of these components at a time to get non-immersion results.

For some component, let m_i be the number associated to the ith factor in the product, that is constructed just like the number m for 4.2.

Proposition 4.6. *The product of complex flag manifolds* $\prod_{i=1}^{k} U(n_i)/\prod_{j=1}^{k_j} U(n_j^i)$ *cannot be immersed in Euclidean space of dimension* $\sum_{i=1}^{k}(4m_i(n-m_i) - 2\beta(n, m_i)) - 1$ *and it cannot be embedded in Euclidean space of dimension* $\sum_{i=1}^{k} 4m_i(n-m_i) - 2\beta(n, m_i)$.

The proof of this result can be found in appendix A.5. Of cource, 4.4 also transfers to this situation and gives upper bounds on the dimension of stably $\mathcal{S}(\mathbb{C}^n)_{H,s}$-complete POVMs.

4.4. Bob-unitary orbit

Let $\alpha \in \mathcal{H}_A \otimes \mathcal{H}_B$, $\langle\alpha|\alpha\rangle = 1$. In this section we investigate pure states of the form

$$\mathcal{S}_B(\alpha) := \left\{ |\beta\rangle\langle\beta| \in \mathcal{S}\left(\mathcal{H}_A \otimes \mathcal{H}_B\right) : \beta = (\mathbb{1} \otimes U)\alpha,\ U \in U\left(\mathcal{H}_B\right)\right\}.$$

Let $\{e_1, \ldots, e_{\dim \mathcal{H}_A}\}$, $\{f_1, \ldots, f_{\dim \mathcal{H}_B}\}$ be orthonormal bases of $\mathcal{H}_A$ respectively $\mathcal{H}_B$ such that

$$\alpha = \sum_{i=1}^{r} \alpha_i e_i \otimes f_i$$

is a Schmidt decomposition, where r is the Schmidt rank of α. Then, $\mathcal{S}_B(\alpha)$ is diffeomorphic to the projective Stiefel manifold $PW_{n,r}$. In order to see this, note that $(\mathbb{1} \otimes U(\mathcal{H}_B))\alpha$ is diffeomorphic to the complex Stiefel manifolds $W_{n,r} := \{m \in \mathbb{C}^{d\times r} : m^* \cdot m = \mathbb{1}\}$ via

$$i : (\mathbb{1} \otimes U(\mathcal{B}))\alpha \to W_{n,k},$$
$$M_{i,j}\left(\sum_{i=1}^{r} \alpha_i e_i \otimes Uf_i\right) := \left\langle Uf_i \middle| f_j \right\rangle.$$

Factoring both sides over the free action of the cyclic group $S^1 \subseteq \mathbb{C}$, $m \mapsto z \cdot m$, then yields the desired map [20].

In order to state the main result of this section we introduce two functions.

Definition 4.7. Let $n, k \in \mathbb{N}$ and $n \geqslant k$.

1. $N(n, k) := \min\left\{n - k < i \leqslant n : \binom{n}{i} (\mathrm{mod}\ \ 2) \equiv 1\right\}$,
2. $\sigma(n, k) := 2 \cdot \max\left\{0 \leqslant i < N(n, k) : \binom{nk + i - 1}{i} (\mathrm{mod}\ \ 2) \equiv 1\right\}$.

Proposition 4.8. *Let* $\alpha \in \mathcal{H}_A \otimes \mathcal{H}_B$, $\langle\alpha|\alpha\rangle = 1$, *with Schmidt rank* k *and* $n = \dim \mathcal{H}_B$. *Then* $\mathcal{S}_B(\alpha)$ *cannot be immersed in Euclidean space of dimension* $(2n-k)k - 1 + \sigma(n, k)$ *and cannot be embedded in Euclidean space of dimension* $(2n-k)k - 1 + \sigma(n, k) + 1$.

The proof of this result is very similar to [24] and can be found in appendix A.6. This non-immersion result is obtained deploying a standard approach based on the dual Stiefel–Whitney class of the tangent bundle [25].

For $k = 1$ the complex projective Stiefel manifold is just the complex projective space, so in this chase we can compare the result obtained here to the upper bounds of Milgram [26], which are known to be close to optimal. Table 2 shows these bounds for some dimensions.

For $n = 2^k$, $k \in \mathbb{N}$, the dual Stiefel–Whitney classes give no obstructions, whereas they essentially equal Milgram's result in [26] for $n = 2^k + 1$, $k \in \mathbb{N}$, and hence are close to optimal in this case.

In [27], it is shown that $PW_{n,n}$ and $PW_{n,n-1}$ is parallelizable for $n \neq 2$ and thus can be immersed in Euclidean space of codimension one by a result of Hirsch [28]. For $PW_{4,k}$ and $PW_{8,k}$, there are no obstructions because the dual Stiefel–Whitney classes vanish for $nk = q2^r$, $q, r \in \mathbb{Z}$ and $N(n, k) < 2^r$ [24].

In table 3 these bounds are presented for some explicit scenarios. The dual Stiefel–Whitney classes do not generally give good obstructions, but can be supplemented by other methods. Another approach to the non-immersion problem is due to [29]. In a similar vein, another method is given to obtain non-immersion results, with the exterior powers γ_i of $KO(X)$ playing the role of the Stiefel–Whitney classes. Both of these methods are worked out and compared in [24].

Next, we give upper bounds on the dimension of an $S_B(\alpha)$-embedding, presenting two different approaches.

The first approach is based on the upper bounds obtained for states of fixed spectrum. The problem is split into determining the minor obtained by tracing over $\mathcal{H}_A$ and afterwards determining the relative phases.

Before stating the upper bounds, let us first prove the following lemma which will be useful later on.

Lemma 4.9. *Let* $\alpha := \sum_{i=1}^{r} \lambda_i e_i \otimes f_i$, $O \in H(\mathcal{H}_A)$, $S \in H(\mathcal{H}_B)$, $U \in U(\mathcal{H}_B)$ *and* $P_\alpha := \sum_{i=1}^{r} \lambda_i |e_i\rangle\langle f_i|$. *Then* $\mathrm{tr}(O \otimes USU^\dagger |\alpha\rangle\langle\alpha|) = \mathrm{tr}((P_\alpha U)^\dagger O^T (P_\alpha U) S)$.

Proof. The prove of this is a straightforward computation

$$\begin{aligned}
\mathrm{tr}\left(O \otimes USU^\dagger |\alpha\rangle\langle\alpha|\right) &= \langle\alpha| O \otimes USU^\dagger |\alpha\rangle \\
&= \sum_{i,j=1}^{r} \lambda_i \lambda_j \langle e_i| \otimes \langle f_i| O \otimes USU^\dagger |e_j\rangle \otimes |f_j\rangle \\
&= \sum_{i,j=1}^{r} \lambda_i \lambda_j \langle e_i| O |e_j\rangle \langle f_i| USU^\dagger |f_j\rangle \\
&= \sum_{i,j=1}^{r} \lambda_j \langle e_j| O^T |e_i\rangle \lambda_i \langle f_i| USU^\dagger |f_j\rangle \\
&= \sum_{i,j=1}^{r} \langle f_i | f_j\rangle \lambda_j \langle e_j| O^T P_\alpha USU^\dagger |f_i\rangle \\
&= \sum_{i=1}^{r} \langle f_i| U^\dagger P_\alpha^\dagger O^T P_\alpha US |f_i\rangle \\
&= \mathrm{tr}\left((P_\alpha U)^\dagger O^T (P_\alpha U) S\right).
\end{aligned}$$

□

The following proposition is motivated by a method to embed Lie groups in Euclidean space, introduced in [30].

Proposition 4.10. *Let $\alpha \in \mathcal{H}_A \otimes \mathcal{H}_B$ with Schmidt rank* k *and* $n = \dim \mathcal{H}_B$. *Then, there is a $S_B(\alpha)$-embedding of dimension $4r(n-r) - 1 + 4n - 5$ for $r < n/2$ and $n^2 - 1 + 4n - 5$ for $r \geqslant d/2$.*

Proof. First, note that by lemma 4.9 we can assume w.l.o.g. that $\lambda_i \neq \lambda_j$ for $1 \leqslant i, j \leqslant r$, $i \neq j$, because this can always be achieved by choosing O appropriately.

The idea is to take advantage of the natural projection $\pi : PW_{n,r} \to \dfrac{U(n)}{U(1)^r \times U(n-r)}$, which just amounts to choosing $O = \mathbb{1}$ in lemma 4.9. More precisely, for $O = \mathbb{1}$ we get

$$P_\alpha O P_\alpha^\dagger = \begin{pmatrix} \lambda_1 & & & & \\ & \ddots & & & \\ & & \lambda_r & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

and thus we are in the situation discussed in the last section with the isotropy group given by $U(1)^r \times U(n-r)$. This means, the projected state can be embedded in dimension $4r(d-r) - 1$ using the POVM of 4.4. Let us call this map ϕ_1.

Let $v \in \mathbb{C}^r$ be the vector with a one in every entry and consider the map

$$\begin{aligned} \psi\colon U(n)/U(n-r) &\to \mathbb{C}^n, \\ U &\mapsto U(v \oplus 0). \end{aligned}$$

This is clearly well defined and also observe that ψ descents to a map $\tilde{\psi} : PW_{n,r} \simeq U(n)/(U(n-r) \times U(1)) \to P\mathbb{C}^n$. Let $U, V \in U(n)$ with $U \sim V$ in $U(n)/U(1)^r \times U(n-r)$, i.e. $U = V(D \oplus \mathbb{1})(\mathbb{1} \oplus W)$ with $D \in U(1)^r$ and $W \in U(n-r)$. Then, $Uv = \lambda Vv$ just has a solution for $U \sim V$ in $U(n)/(U(1) \times U(n-r))$. To see this, note that

$$\begin{aligned} U(v \oplus 0) &= \lambda V(v \oplus 0) \\ V(D \oplus \mathbb{1})(\mathbb{1} \oplus W)(v \oplus 0) &= \lambda V(v \oplus 0) \\ (D \oplus \mathbb{1})(v \oplus 0) &= \lambda(v \oplus 0) \\ Dv &= \lambda v \end{aligned}$$

and thus $D = \lambda \mathbb{1}$ is the only solution.

Hence, supplementing the embedding above by $\tilde{\psi}$ guarantees injectivity and the only problem left, is embedding $P\mathbb{C}^n$.

In terms of lemma 4.9 $\tilde{\psi}$ corresponds to choosing $P_\alpha O^T P_\alpha^\dagger = v^\dagger v \oplus 0$, the projective version of $v \oplus 0$. Then choose S according to the POVM of [2] to obtain an embedding in Euclidean space. Let us call this mapping ϕ_2

The map $\phi := (\phi_1, \phi_2)$ is clearly smooth as well as injective and thus a topological embedding by compactness of $S_B(\alpha)$. From lemma 4.9 it is easy to see that $\frac{\mathrm{d}}{\mathrm{d}t}|_{t=0}(\mathbb{1} \otimes U\mathrm{e}^{\mathrm{i}Ht})|\alpha\rangle\langle\alpha|(\mathbb{1} \otimes \mathrm{e}^{-\mathrm{i}Ht}U^\dagger)$ for $H = h \oplus 0$ and $h \neq \mathbb{1}$ diagonal gives a $n-1$ dimensional subspace V_U of the tangent space at $\alpha_U := (\mathbb{1} \otimes U)|\alpha\rangle\langle\alpha|(\mathbb{1} \otimes U^\dagger)$. V_U is clearly in the kernel of $d\phi_1|_{\alpha_U}$. Thus, by dimensional reasoning, it is enough to see that $d\phi_2|_{\alpha_U}$ is injective on V_U. Since the POVM of [2] can identify all rank one matrices, it is enough to see that $h \oplus 0 \mapsto [v\dagger v \oplus 0, h \oplus 0]$ is injective for $h \neq \mathbb{1}$ diagonal. This can be easily verified by a direct computation. □

Remark. This result is best for r close to n, so in particular for $PW_{n,n}$, the set of maximally entangled states. For $PW_{n,n}$ we obtain an embedding in Euclidean space of codimension $4n - 5$.

Furthermore, note that in the context of quantum process tomography, the result for maximally entangled states can be used to identify a unitary time evolution. Preparing a certain maximally entangled state, the POVM given above can identify unitary processes up to a phase, i.e. with $\mathcal{O}(n^2)$ measurements.

The second approach relies on the direct construction of an $S_B(\alpha)$-embedding.

Proposition 4.11. *Let $\alpha \in \mathcal{H}_A \otimes \mathcal{H}_B$ with Schmidt rank* r *and $n = \dim \mathcal{H}_B$. Then, there is a $S_B(\alpha)$-embedding of dimension $2nr + 2n - 3$.*

Proof. First, note that w.l.o.g. we can assume $\lambda_1 = \cdots = \lambda_r = 1$, as can be easily seen from lemma 4.9.

Then, for $O = |e_i\rangle\langle e_j|$, $S = |f_k\rangle\langle f_l|$ we obtain

$$\mathrm{tr}\Big(\big(P_\alpha U\big)^\dagger O^T \big(P_\alpha U\big) S \Big) = \big\langle f_i \big| U \big| f_k \big\rangle \big\langle f_j \big| U \big| f_l \big\rangle^*,$$

so from this point of view any linear combination of such products of elements of $P_\alpha U$ determines an operator, that need not be hermitian, and a set of such equations determines an operator system (here we think of $P_\alpha U$ as a matrix in the $\{e_i\}_{i\in\{1,\ldots r\}}$, $\{f_l\}_{l\in\{1,\ldots n\}}$ basis). It is worth noting that an equation not corresponding to a non-hermitian operator actually corresponds to two operators in the operator system, namely its hermitian and anti-hermitian part.

Let $M_{n(i-1)+j}(U) \coloneqq \langle e_i| P_\alpha U |f_j\rangle$ for $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, n\}$ and $M_k \coloneqq 0$ for $k > nr$. For $k \in \{1, \ldots, nr + n - 1\}$, define operators $\tilde{G}_k$ via the equations

$$G_k(U) \coloneqq \sum_{i=1, i\leqslant k+1-i}^{n} M_i(U) M^*_{k+1-i}(U).$$

Then, the operator system σ_G spanned by the $\tilde{G}_k$ is an $S_B(\alpha)$-embedding. It is clear that the dimension of σ_G is $2nr + 2n - 3$, noting that non-hermitian operators count twice.

Let $U, V \in U(\mathcal{H}_B)$. In order to prove injectivity, we have to show that if $G_k(U) = G_k(V)$, then there is a $\phi \in \mathbb{R}$ such that $P_\alpha U = \mathrm{e}^{\mathrm{i}\phi} P_\alpha V$. First, observe that for $M_1(U) = \cdots = M_k(U) = 0$ we have $k \leqslant n$ because $P_\alpha U$ has full rank. Let m be the smallest number such that M_m does not vanish. Then the claim is clearly true for all $j < m$. Now, let $l > m$ and assume that the claim holds for all $j \leqslant l$, then

$$\begin{aligned} G_{m+l}(U) &= \sum_{i=1, i\leqslant m+l+1-i}^{n} M_i(U) M^*_{m+l+1-i}(U) \\ &= M_m(U) M_{l+1}(U)^* + \sum_{i=m+1, i\leqslant m+l+1-i}^{n} M_i(U) M^*_{m+l+1-i}(U) \\ &= M_m(V) \mathrm{e}^{\mathrm{i}\phi} M_{l+1}(U)^* + \sum_{i=m+1, i\leqslant m+l+1-i}^{n} M_i(V) M^*_{m+l+1-i}(V) \\ &= G_{m+l}(V), \end{aligned}$$

thus $\mathrm{e}^{-\mathrm{i}\phi} M_{l+1}(U) = M_{l+1}(V)$.

Table 4. Dimension/Lower bounds on immersion dimension 4.8; first upper bound on embedding dimension 4.10; second upper bound on embedding dimension 4.11 for $PW_{n,r}$.

$n\backslash r$	5	9	17	65
5	24/24;40;57			
9	64/70;112;105	80/80;112;177		
17	144/166;302;201	224/238;352;337	288/288;352;609	
65	624/742;1454;777	1088/ 1198;2270;1297	1920/ 2014;3518;2337	4224/4224;4480;8577
129	1264/ 1510;2990;1545	2240/ 2478;4830;2577	4096/ 4318;8126;4641	12544/ 12670;17152;17025

To conclude the proof, we need to show that the measurement constructed above is an immersion. For $h \in H(\mathcal{H}_B)$, $U \in U(\mathcal{H}_B)$ and and define a curve $\gamma(t) := (\mathbb{1} \otimes e^{iUhU^\dagger t}U)|\alpha\rangle\langle\alpha|(\mathbb{1} \otimes U^\dagger e^{-iUhU^\dagger t})$. The derivative of this curve yields tangent vectors at $(\mathbb{1} \otimes U)|\alpha\rangle\langle\alpha|(\mathbb{1} \otimes U^\dagger)$ and by lemma 4.9 an effect operator $O \otimes S$ maps these to

$$\frac{\mathrm{d}}{\mathrm{d}t}|_{t=0}\,\mathrm{tr}\left(\left(P_\alpha e^{iUhU^\dagger t}U\right)^\dagger O^T\left(P_\alpha e^{-iUhU^\dagger t}U\right)S\right)$$
$$= i\mathrm{tr}\left(P_\alpha^\dagger O^T P_\alpha U[h, S]U^\dagger\right).$$

For $k \in \{1, \ldots, nr + n - 1\}$, this yields the equations

$$F_k(U, h) = \sum_{i=1, i\leqslant m+l+1-i}^{n} M_i(U)M^*_{k+1-i}(Uh) - M_i(Uh)M^*_{k+1-i}(U).$$

Observe that $F_k(U, h) = F_k(U, h + c\mathbb{1})$ holds for each $c \in \mathbb{C}$. Furthermore, it is easy to see that for every $k \in \{1, \ldots, nr\}$ and every $h \in H(\mathcal{H}_B)$ there is a $\lambda \in \mathbb{C}$ such that $M_k(U(\lambda\mathbb{1} + h)) = 0$ and thus we can assume w.l.o.g. that $M_k(Uh) = 0$.

Let m be the smallest number such that $M_m(U)$ does not vanish and assume w.l.o.g. $M_m(Uh) = 0$. Let $l \in \{1, \ldots, nr + m - 1\}$. It is easy to see that the vanishing of these equations for all $i \leqslant l$ implies that $M_j(Uh) = 0$ for $j \leqslant l + 1 - k$ and thus, we obtain injectivity on a real vector space of dimension $2nr - r^2 - 1$. □

In table 4 both of these methods are compared. It is clear that the embedding in 4.11 works best for $k/m \ll 1$, because this approach does not take the orthogonality of the f_i into account. The embedding in 4.10 works best for $k/m \sim 1$, because just in this case the projected state can be determined efficiently.

Appendix A. Technical appendix

A.1. Proof of theorem 3.3

Before we give the proof, let us first fix some notion.

Let $\mathcal{SO}(H(\mathcal{H}))$ be the orthogonal group on the inner product space $H(\mathcal{H})$. The generalized Pauli basis together with the identity $\mathbb{1}_\mathcal{H}$ gives an identification of $H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$ and the Hilbert–Schmidt inner product induces the standard inner product on $\mathbb{R}^{d^2}$. Thus $\mathcal{SO}(H(\mathcal{H}))$ can be identified with $\mathcal{SO}(\mathbb{R}^{d^2})$, the standard orthogonal group on $\mathbb{R}^{d^2}$. Denote by

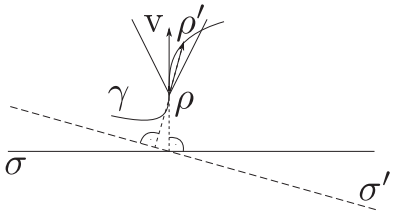

Figure A1. This figure shows the curve γ with $\gamma(0) = \rho$, $\gamma(t') = \rho'$ and $\frac{\mathrm{d}}{\mathrm{d}t}\gamma(0) = v \in \sigma^{\perp}$ together with the operator system σ' that is constructed such that $\rho' - \rho \in (\sigma')^{\perp}$.

$\mathcal{SO}(H(\mathcal{H}))_v \coloneqq \{O \in \mathcal{SO}(H(\mathcal{H})) : Ov = v\}$ the stabilizer subgroup of $v \in H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$. Note that for $O \in \mathcal{SO}(H(\mathcal{H}))_{\mathbb{1}_{\mathcal{H}}}$ and $\sigma \in \Sigma(n)$, we have $O\sigma \in \Sigma(n)$. Thus there is an action of $\mathcal{SO}(H(\mathcal{H}))_{\mathbb{1}_{\mathcal{H}}}$ on $\Sigma(n)$

$$\begin{aligned}\Sigma(n) \times \mathcal{SO}(H(\mathcal{H}))_{\mathbb{1}_{\mathcal{H}}} &\to \Sigma(n) \times \Sigma(n)\\ (\sigma,\, O) &\mapsto (\sigma,\, O\sigma).\end{aligned}$$

The geometric intuition of thinking of operator systems as planes in $H(\mathcal{H}) \simeq \mathbb{R}^{d^2}$ is essential for the following proof. Then, for $O \in \mathcal{SO}(H(\mathcal{H}))_{\mathbb{1}_{\mathcal{H}}}$, $O\sigma$ is just a rotated plane and the intuition is that for small rotations these operator systems are close.

Proof. Let $\sigma \in \Sigma(n)$ be stably $\mathcal{P}$-complete and π_σ be the associated orthogonal projection. Furthermore let $SH(\mathcal{H}) \coloneqq \{B \in H(\mathcal{H}) : \|B\| = 1\}$ be the unit sphere in $H(\mathcal{H})$. Assume by contradiction that σ is not a $\mathcal{P}$-embedding, i.e. π_σ is not an immersion. Then, since $d(\pi_\sigma)_\rho = \pi_{\sigma T_\rho \mathcal{P}}$, there exists a point $\rho \in \mathcal{P}$ and a smooth curve $\gamma : (-1, 1) \to \mathcal{P}$ with $\gamma(0) = \rho$ and $v = \dot{\gamma}(0) \in \sigma^{\perp}$, $v \in SH(\mathcal{H})$. The idea is that $\gamma(t) \approx \rho + vt$ for small t and to obtain a contradiction we construct for a point $\rho' = \gamma(t') \approx \rho + vt'$ an operator system σ' with $\pi_{\sigma'}(\rho' - \rho) = 0$. This procedure is presented in figure A1.

More precisely, we prove that for each $\delta > 0$ there is a $t \in (0, 1)$ such that $\gamma(t) \in V_\rho^\delta \coloneqq \{\rho + \lambda \cdot Ov :\ \lambda > 0,\, O \in \mathcal{SO}(H(\mathcal{H})),\, \|\mathbb{1} - O\|_{op} < \delta\}$.

First, we prove that V_ρ^δ is open. Note that the left action

$$\begin{aligned}\mathcal{SO}(H(\mathcal{H})) \times SH(\mathcal{H}) &\to SH(\mathcal{H}) \times SH(\mathcal{H})\\ (O,\, v) &\mapsto (Ov,\, v)\end{aligned}$$

is smooth and transitive. Thus, the orbit map $\beta_v : \mathcal{SO}(H(\mathcal{H})) \to SH(\mathcal{H})$, $O \mapsto Ov$ is smooth and factors over the natural projection $\pi : \mathcal{SO}(H(\mathcal{H})) \to \mathcal{SO}(H(\mathcal{H}))/\mathcal{SO}(H(\mathcal{H}))_v$ (theorem 3.62 of [20]), i.e. $\beta_v = \tilde{\beta}_v \circ \pi$ with $\tilde{\beta}_v$ a diffeomorphism. In particular β_v is open because π is open[11].

Since β_v is open there is an $\eta > 0$ such that $\varnothing \neq B_{\rho+v}(\eta) \cap B_\rho(1) \subseteq V_\rho^\delta$. By possibly shrinking η we can even assume that $\overline{B}_{\rho+v}(\eta) \subseteq V_\rho^\delta$ because of the conic structure of V_ρ^δ. It follows that $B_{\rho+sv}(s\eta) \subseteq V_\rho^\delta$ for $s > 0$.

[11] For an open set $A \subseteq \mathcal{SO}(H(\mathcal{H}))$ we find $\pi^{-1}(\pi(A)) = \mathcal{SO}(H(\mathcal{H}))_v \cdot A = \bigcup_{O \in \mathcal{SO}(H(\mathcal{H}))_v} O(A)$. So $\pi^{-1}(\pi(A))$ is open for any open set $A \subseteq \mathcal{SO}(H(\mathcal{H}))$ and thus π is open.

Then

$$\frac{\|\gamma(t) - (\rho + tv)\|}{t} = \frac{\|\gamma(t) - \gamma(0) - tv\|}{t} \to 0 \text{ as } t \to 0,$$

whereas we find for the distance $d(\rho + tv, \partial B_{\rho+tv}(t\eta))/t \coloneqq \inf_{\rho' \in \partial B_{\rho+tv}(t\eta)} \|\rho - \rho'\|/t = \eta$. So by continuity of the norm there is a $t > 0$ such that $\gamma((0, t)) \subseteq V_\rho^\delta$.

But then, for every $\delta > 0$, there is an $O \in \mathcal{SO}(H(\mathcal{H}))$, a $\lambda > 0$ and a $t > 0$ with

$$\begin{aligned} d(\sigma, O\sigma) &= \|\pi_\sigma - \pi_{O\sigma}\|_{op} \\ &= \|\pi_\sigma - O\pi_\sigma O^{-1}\|_{op} \\ &\leqslant \|\pi_\sigma - \pi_\sigma O^{-1}\|_{op} + \|\pi_\sigma - O\pi_\sigma\|_{op} \\ &\leqslant 2\,\|\mathbb{1} - O\|_{op} < 2\delta \end{aligned}$$

such that $\gamma(t) - \gamma(0) = \lambda O v \neq 0$. But then, $\pi_{O\sigma}(\gamma(t) - \gamma(0)) = O\pi_\sigma(O^{-1}(\gamma(t) - \gamma(0))) = \lambda O\pi_\sigma(v) = 0$ by assumption on v. Also note that $\langle \mathbb{1}_\mathcal{H}, \gamma(t) - \gamma(0)\rangle \coloneqq tr[\mathbb{1}_\mathcal{H}(\gamma(t) - \gamma(0))] = 0$ and $\langle \mathbb{1}, T_\rho \mathcal{P}\rangle = 0$ and thus we can choose $O \in \mathcal{SO}(H(\mathcal{H}))_{\mathbb{1}_\mathcal{H}}$. So $O\sigma$ is an operator system but it is not $\mathcal{P}$-complete, contradicting the stability of σ.

Conversely, suppose σ is a $\mathcal{P}$-embedding. A.2 states, that there is an $\epsilon > 0$ such that every $\sigma' \in \Sigma(n)$ with $\sup_{B \in H(\mathcal{H}), \|B\| \leqslant 1} \|\pi_\sigma(B) - \pi_{\sigma'}(B)\| < \epsilon$ is a $\mathcal{P}$-embedding and thus in particular $\mathcal{P}$-complete.. □

A.2. Proof of lemma 3.5

The following proof uses geometric concepts and is based on the identification of the tangent spaces with planes in $H(\mathcal{H})$.

Proof. π^T is smooth, as can be easily seen in local coordinates. The mapping

$$\begin{aligned} \psi : \mathcal{P} \times \mathcal{P} &\to \mathbb{R} \\ (\rho', \rho) &\mapsto \|\pi_{\rho'}^T - \pi_\rho^T\|_{op} \end{aligned}$$

is clearly continuous as a composition of continuous mappings and thus, for every $\eta > 0$, there is an open neighbourhood N_{ρ_0} of $\rho_0 \in \mathcal{P}$ such that $\psi(\rho, \rho_0) < \eta/4$ for all $\rho \in N_{\rho_0}$. Let $\nu_0 > 0$ and let $B_{5\nu_0}(\rho_0)$ be the open ball of radius $5\nu_0$ around ρ_0, such that $B_{5\nu_0}(\rho_0) \cap \mathcal{P}$ is contained in N_{ρ_0}.

Let $\rho \in B_{\nu_0}(\rho_0) \cap \mathcal{P}$. Then, for all $\tilde{\rho} \in B_{4\nu_0}(\rho) \cap \mathcal{P}$, we find

$$\psi(\rho, \tilde{\rho}) < \psi(\rho, \rho_0) + \psi\left(\tilde{\rho}, \rho_0\right) < \eta/2. \tag{A.1}$$

Let $\rho' \in \partial B_\epsilon(\rho) \cap \mathcal{P}$, $0 < \epsilon < \nu_0$. Furthermore, let $\gamma : [0, \lambda] \to \mathcal{P} \subseteq S(\mathcal{H})$ be a geodesic that connects ρ and ρ' with $\gamma(0) = \rho$ and $\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)|_{t=0} = v$, $\|v\| = 1$. Since $(\rho, v) \mapsto \frac{\mathrm{d}^2}{\mathrm{d}t^2}\gamma(t)|_{t=0} = \frac{\mathrm{d}^2}{\mathrm{d}t^2}\exp(\rho, vt)|_{t=0}$ is a smooth function from the compact set $\mathcal{P} \times S^{\dim \mathcal{P}-1}$ to $H(\mathcal{H})$, there is $k \geqslant 0$ such that $k \coloneqq \max_{(\rho,v) \in \mathcal{P} \times S^{\dim \mathcal{P}-1}} \|\dfrac{\mathrm{d}^2}{\mathrm{d}t^2}\exp(\rho, vt)|_{t=0}\|$. It follows from the geodesic equation

$$\pi^T_{\gamma(t)}\left(\frac{\mathrm{d}^2}{\mathrm{d}t^2}\gamma(t)\right) = 0,$$

$$\pi^T_{\gamma(0)}\left(\frac{\mathrm{d}^2}{\mathrm{d}t^2}\gamma(t)\right) + \left(\pi^T_{\gamma(t)} - \pi^T_{\gamma(0)}\right)\left(\frac{\mathrm{d}^2}{\mathrm{d}t^2}\gamma(t)\right) = 0,$$

$$\pi^T_{\gamma(0)}\left(\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)\right) + \int_0^t \mathrm{d}t'\left(\pi^T_{\gamma(t')} - \pi^T_{\gamma(0)}\right)\left(\frac{\mathrm{d}^2}{\mathrm{d}t'^2}\gamma(t')\right) = v,$$

$$\pi^T_{\gamma(0)}(\gamma(t)) + \int_0^t \mathrm{d}t' \int_0^{t'} \mathrm{d}t''\left(\pi^T_{\gamma(t'')} - \pi^T_{\gamma(0)}\right)\left(\frac{\mathrm{d}^2}{\mathrm{d}t''^2}\gamma(t'')\right) = vt + \pi^T_{\gamma(0)}(\rho).$$

However, for $t \in [0, 4\nu_0]$

$$\begin{aligned}
&\left\| \int_0^t \mathrm{d}t'\left(\pi^T_{\gamma(t')} - \pi^T_{\gamma(0)}\right)\left(\frac{\mathrm{d}^2}{\mathrm{d}t'^2}\gamma(t')\right)\right\| \\
&\leqslant \int_0^t \mathrm{d}t' \left\| \left(\pi^T_{\gamma(t')} - \pi^T_{\gamma(0)}\right)\left(\frac{\mathrm{d}^2}{\mathrm{d}t'^2}\gamma(t')\right)\right\| \\
&< \int_0^t \mathrm{d}t' k\eta \Big/ 2 = kt\eta \Big/ 2 \leqslant 2\eta k\nu_0.
\end{aligned}$$

as well as

$$\begin{aligned}
&\left\| \int_0^t \mathrm{d}t' \int_0^{t'} \mathrm{d}t''\left(\pi^T_{\gamma(t'')} - \pi^T_{\gamma(0)}\right)\left(\frac{\mathrm{d}^2}{\mathrm{d}t''^2}\gamma(t'')\right)\right\| \\
&\leqslant \int_0^t \mathrm{d}t' \int_0^{t'} \mathrm{d}t'' \left\| \left(\pi^T_{\gamma(t'')} - \pi^T_{\gamma(0)}\right)\left(\frac{\mathrm{d}^2}{\mathrm{d}t''^2}\gamma(t'')\right)\right\| \\
&< \int_0^t \mathrm{d}t' \int_0^{t'} \mathrm{d}t'' k\eta \Big/ 2 = kt^2\eta \Big/ 4 \leqslant 4\eta k(\nu_0)^2.
\end{aligned}$$

Thus, we find

$$\left\|\pi^T_{\gamma(0)}(\gamma(t) - (vt + \rho))\right\| < kt^2\eta \Big/ 4 < 4\eta k(\nu_0)^2$$

and

$$\begin{aligned}
\left\|\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t) - v\right\| &= \left\|\pi^T_{\gamma(t)}\left(\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)\right) - \pi^T_{\gamma(0)}\left(\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)\right) + \pi^T_{\gamma(0)}\left(\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)\right) - v\right\| \\
&\leqslant \left\|\pi^T_{\gamma(t)}\left(\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)\right) - \pi^T_{\gamma(0)}\left(\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)\right)\right\| + \left\|\pi^T_{\gamma(0)}\left(\frac{\mathrm{d}}{\mathrm{d}t}\gamma(t)\right) - v\right\| \\
&\leqslant \eta/2 + 2\eta k\nu_0,
\end{aligned}$$

Note that γ stays inside $B_{5\nu_0}(\rho_0)$. Furthermore, for η and ν_0 small enough, γ intersects $\partial B_{2\nu_0}(\rho_0)$ and γ intersects $\partial B_\epsilon(\rho)$ close to radial. In particular it follows that $t \mapsto \|\gamma(t) - \rho\|$ is strictly increasing as long as γ stays inside $B_{2\nu_0}(\rho_0)$. Then, each geodesic intersects $\partial B_\epsilon(\rho)$ exactly once before it passes through $\partial B_{2\nu_0}(\rho_0)$ for each ϵ with $0 < \epsilon < \nu_0$. Let K_ρ be the connected component of $\mathcal{P} \cap B_{\nu_0}(\rho)$ containing ρ and let K_{ρ_0} be the connected component of $\mathcal{P} \cap B_{2\nu_0}(\rho_0)$ containing ρ_0. The above reasoning implies that $K_\rho \cap B_\epsilon(\rho)$ is connected and that $K_{\rho_0} \cap B_{\tilde{\epsilon}}(\rho_0)$ is connected for $0 < \tilde{\epsilon} < 2\nu_0$.

We can assume w.l.o.g. that $B_{\nu_0}(\rho) \cap \mathcal{P}$ is connected for all $\rho \in B_{\nu_0}(\rho_0)$. Because if not, we can shrink ν_0 until $B_{2\nu_0}(\rho_0)$ contains a single connected component. To see this, shrink ν_0 such that $0 < \nu_0 < \max_{\rho \in \overline{K_{\rho_0}}, \rho' \in (\overline{B_{2\nu_0}}(\rho_0) \cap \mathcal{P}) - \overline{K_{\rho_0}}} \|\rho - \rho'\|$.

We then find for $0 < \epsilon < \nu_0$ and $t \in [0, 4\epsilon]$

$$\begin{aligned}\|\pi^T_{\gamma(0)}(\gamma(t) - \rho)\| &= \|\pi^T_{\gamma(0)}(\gamma(t) - (vt + \rho)) + vt)\| \\ &> \|vt\| - \|\pi^T_{\gamma(0)}(\gamma(t) - (vt + \rho))\| > t - 4\eta k\epsilon^2.\end{aligned}$$

Hence, $\gamma(t) = \rho'$ and $\gamma([0, t]) \subseteq B_{2\nu_0}(\rho_0) \Rightarrow t < \epsilon + 4\eta k\epsilon^2$.

Choosing ν_0 such that $4\,k\nu_0 < 1$, we find for the component of $\rho' - \rho = \gamma(t) - \gamma(0)$ normal to $T_\rho\mathcal{P}$

$$\begin{aligned}\left\|\pi^N_\rho(\rho' - \rho)\right\| &= \left\| \int_0^t \mathrm{d}t' \frac{\mathrm{d}}{\mathrm{d}t'}\gamma(t') - \pi^T_{\gamma(0)}\left(\frac{\mathrm{d}}{\mathrm{d}t'}\gamma(t')\right)\right\| \\ &\leqslant \int_0^t \mathrm{d}t' \left\| \pi^T_{\gamma(t')}\left(\frac{\mathrm{d}}{\mathrm{d}t'}\gamma(t')\right) - \pi^T_{\gamma(0)}\left(\frac{\mathrm{d}}{\mathrm{d}t'}\gamma(t')\right)\right\| \\ &< \int_0^t \mathrm{d}t' \eta \Big/ 2 = t\eta \Big/ 2 < \eta(\epsilon + 4\,k\epsilon^2) \Big/ 2 \leqslant \epsilon\eta(1 + 4\,k\nu_0) \Big/ 2 < \eta\epsilon \\ &= \eta\,\|\rho - \rho'\|.\end{aligned}$$

Now, for a given $\eta > 0$, construct such neighbourhoods for all $\rho \in \mathcal{P}$ to obtain a cover of $\mathcal{P}$ by open sets, $\{B_{\nu_\rho}(\rho) \cap \mathcal{P}\}_{\rho \in \mathcal{P}}$. By compactness of $\mathcal{P}$ there is a finite subcover $\{B_{\nu_{\rho_i}}(\rho_i) \cap \mathcal{P}\}_{i \in I}$ and set $\epsilon := \min_{i \in I} \nu_{\rho_i}$. □

Remark. Note that the proof of this lemma shows that for $0 < \tilde{\epsilon} < \epsilon$, $B_{\tilde{\epsilon}}(\rho) \cap \mathcal{P}$ is connected.

A.3. Proof of proposition 3.10

Proof. To see that i is smooth, choose an orthonormal basis $\{\sigma_i\}_{i \in I}$ of hermitian operators for $H(\mathcal{H})$. Expansion in this basis gives global coordinates on $H(\mathcal{H})$. Expansion in $\{\sigma_{i_1} \otimes \cdots \otimes \sigma_{i_k}\}_{i_1, \ldots, i_k \in I}$ gives global coordinates on $H(\mathcal{H})^{\otimes k}$. In these coordinates i is just a polynomial and hence smooth.

$\mathcal{P}$ is a smooth submanifold and since $\mathcal{P} \subseteq S(\mathcal{H}) \subseteq H(\mathcal{H})$, $i_{\mathcal{P}}$ is smooth. We prove that $i|_{\mathcal{P}}$ is injective. Note that $\rho^{\otimes k} = \sigma^{\otimes k}$ iff $\sigma = a \cdot \rho$, $a^k = 1$. But then $\sigma, \rho \in H(\mathcal{H})$ implies $a \in \{-1, 1\}$ and the positivity of both σ and ρ yields $a = 1$.

Finally, $i|_{\mathcal{P}}$ is an immersion. To see this let $\rho \in \mathcal{P}$ and $v \in T_\rho\mathcal{P}$. Furthermore, let $\gamma\colon (-1, 1) \to H(\mathcal{H})$ be a smooth curve with $\gamma(0) = \rho$ and $\frac{\mathrm{d}}{\mathrm{d}t}\gamma(0) = v$. First, observe that for $k = 2$

$$\begin{aligned}\mathrm{d}i_\rho v = \frac{\mathrm{d}}{\mathrm{d}t}\Big|_{t=0}(i \circ \gamma) &= \lim_{t \to 0} \frac{\gamma(t)^{\otimes 2} - \gamma(0)^{\otimes 2}}{t} \\ &= \lim_{t \to 0} \frac{(\gamma(t) - \gamma(0)) \otimes \gamma(t) - (\gamma(0) - \gamma(t)) \otimes \gamma(0)}{t} = \rho \otimes v + v \otimes \rho.\end{aligned}$$

This inductively generalizes to arbitrary $k \in \mathbb{N}$ and we get

$$\mathrm{d}i_\rho v = \sum_{i=1}^{k} \rho^{\otimes i-1} \otimes v \otimes \rho^{\otimes k-i}.$$

This is zero if and only if $v = 0$, what can be easily seen by orthogonally decomposing v with respect to ρ.

Finally, since $i_{\mathcal{P}}$ is smooth, injective and an immersion, it is a smooth embedding by the compactness of $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$. □

Remark. Note that the proof shows that $i_{H(\mathcal{H})-\{0\}}$ is an immersion.

A.4. Proof of lemma 3.13

In this lemma we prove that, for a submanifold $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$, every smooth embedding $\psi : \mathcal{P} \to \mathbb{R}^m$ can be approximated by a polynomial map $F : \mathbb{1}_{\mathcal{H}} + H_0(\mathcal{H}) \simeq \mathbb{R}^{d^2-1} \to \mathbb{R}^m$. Let us first state lemma 1.3 of [31].

Lemma A.1. *[31] Let $U \subseteq \mathbb{R}^n$ be open and $W \subseteq U$ be open with compact closure $\overline{W} \subseteq U$. Let $f : U \to \mathbb{R}^n$ be a smooth embedding. There exists $\epsilon > 0$ such that if $g : U \to \mathbb{R}^n$ is smooth and*

$$\| D_\alpha g(x) - D_\alpha f(x) \|_2 < \epsilon \quad \text{and} \quad \| g(x) - f(x) \|_2 < \epsilon$$

for all $x \in W$, $|\alpha| = 1$, then $g\,|_W$ is an embedding.

Now we give the proof of lemma 3.13.

Proof. Note that $\psi' = \tilde{\psi}'_{\mathcal{P}}$ is smooth because it is a restriction of smooth functions to a smooth submanifold. ψ can be extended to a compactly supported smooth map $\tilde{\psi}$ on $\mathbb{1}_{\mathcal{H}} + H(\mathcal{H})_0 \simeq \mathbb{R}^{n^2-1}$ and let $K \subseteq \mathbb{R}^{n^2-1}$ be a compact set containing $\operatorname{supp} \tilde{\psi}$. In the following we make use of an approximation result given by theorem 1 in [32]. The relevant part for us is that for every $\eta > 0$, there is a $k \in \mathbb{N}$ such that $\tilde{\psi}$ and $d\tilde{\psi}$ can be approximated simultaneously by a map $\tilde{\psi}' = (p_1, \ldots, p_i)$, $p_i \in P^{\leqslant k}(\mathbb{R}^{n \times n-1})$, i.e $\sup_{x \in K} \| \tilde{\psi}(x) - \tilde{\psi}'(x) \|_2 < \eta$ and $\sup_{(x,v) \in TK, \|v\| \leqslant 1} \| d\tilde{\psi}_x(v) - d\tilde{\psi}'_x(v) \|_2 < \eta$.

Let $\{ (\phi_i, W_i) \}_{i \in I}$ be a finite atlas on $\mathcal{P}$ and let $\tilde{B}(r_i) \coloneqq \phi_i(B(r_i)) \subseteq W_i$ be the image of an open ball of radius r_i around the origin such that $\bigcup_{i \in I} \tilde{B}(r_i/2) = \mathcal{P}$ and $\overline{\tilde{B}(r_i)} \subseteq W_i$. Applying lemma 1.3 of [31] to $\psi \circ \phi_i$, $\phi^{-1}(W_i)$ and $B(r_i)$, we obtain for each $i \in I$ an $\epsilon_i > 0$ such that for all ψ' with $\sup_{B(r_i)} \| D_\alpha(\psi \circ \phi_i) - D_\alpha(\psi' \circ \phi_i) \|_2 < \epsilon_i$, $|\alpha| \leqslant 1$, $\psi'\,|_{\tilde{B}(r_i)}$ is an embedding.

For $|\alpha| = 1$, we have

$$\begin{aligned}
&\sup_{x \in B(r_i)} \| D_\alpha\big(\psi \circ \phi_i\big)(x) - D_\alpha\big(\psi' \circ \phi_i\big)(x) \|_2 \\
&\quad = \sup_{x \in B(r_i)} \| \Big(\mathrm{d}\psi_{\phi(x)} - \mathrm{d}\psi'_{\phi(x)} \Big) \circ D_\alpha \phi_i(x) \|_2 \\
&\quad \leqslant \sup_{(x,v) \in T\tilde{B}(r_i), \|v\| \leqslant 1} \| \Big(\mathrm{d}\psi_x - \mathrm{d}\psi'_x \Big) v \|_2 \sup_{B(r_i)} \| D_\alpha \phi_i \|_2 \\
&\quad \leqslant \sup_{(x,v) \in TK, \|v\| \leqslant 1} \| \Big(\mathrm{d}\tilde{\psi}_x - \mathrm{d}\tilde{\psi'}_x \Big) v \|_2 \sup_{B(r_i)} \| D_\alpha \phi_i \|_2 .
\end{aligned}$$

For $|\alpha| = 1$, let $\kappa_{i,\alpha} \coloneqq \epsilon_i / \sup_{B(r_i)} \| D_\alpha \phi_i \|_2$ and let $\epsilon \coloneqq \min_{i,|\alpha|=1} \{ \epsilon_i, \kappa_{i,\alpha} \}$. Then, for every $\tilde{\psi}'$ with $\sup_{x \in K} \| \tilde{\psi}(x) - \tilde{\psi}'(x) \|_2 < \epsilon$ and $\sup_{(x,v) \in TK, \|v\| \leqslant 1} \| d\tilde{\psi}_x(v) - d\tilde{\psi}'_x(v) \|_2 < \epsilon$, $\tilde{\psi}'_{\tilde{B}(r_i)}$ is an embedding for all $i \in I$ and by theorem 1 of [32] such a $\tilde{\psi}'$ exists for some $k \in \mathbb{N}$.

Finally we show that there is an $\epsilon \geqslant 0$ such that for every $\tilde{\psi}'$ with $\|D_\alpha\tilde{\psi} - D_\alpha\tilde{\psi}'\| < \epsilon$, $\psi'|_{\mathcal{P}}$ is injective. Then ψ' is both an immersion and injective and thus a smooth embedding by the compactness of $\mathcal{P}$.

$\tilde{B}(r_i)^c := \mathcal{P} - \tilde{B}(r_i)$ and $\overline{\tilde{B}(r_i/2)}$ are closed and therefore compact as closed subsets of a compact set. Then, by the continuity of the norm, $\eta_i := \min_{q\in\tilde{B}(r_i)^c, p\in\overline{\tilde{B}(r_i/2)}} \|\psi(p) - \psi(q)\|$ exists and it is bigger than 0 because ψ is injective and $\tilde{B}(r_i)^c \cap \tilde{B}(r_i/2) = \varnothing$. By possibly shrinking ϵ, make sure that $\epsilon \leqslant \frac{1}{4}\min_{i\in I}\eta_i$.

Assume $\psi'(p) = \psi'(q)$, $p, q \in \mathcal{P}$. Since $\psi'|_{\mathcal{P}}$ is an embedding around p, there is an $i \in I$ such that $p \in \tilde{B}(r_i/2)$ and $p \in \tilde{B}(r_i)^c$. Thus

$$\begin{aligned}\|\psi'(p) - \psi'(q)\|_2 &= \|\psi(p) - \psi(q) + \psi'(p) - \psi(p) + \psi(q) - \psi'(q)\|_2\\ &\geqslant |\|\psi(p) - \psi(q)\|_2 - \|\tilde{\psi}'(p) - \tilde{\psi}(p) + \tilde{\psi}(q) - \tilde{\psi}'(q)\|_2\\ &\geqslant 4\epsilon - 2\epsilon > 0,\end{aligned}$$

a contradiction. □

A direct consequence of this proof is the following corollary, which was used in the third section.

Corollary A.2. *Let $\mathcal{P} \subseteq \mathcal{S}(\mathcal{H})$ be a submanifold and let $L : H(\mathcal{H}) \to \mathbb{R}^m$ be a linear map such that $L|_{\mathcal{P}}$ is a smooth embedding. Then, there is an $\epsilon > 0$ such that for every linear map $L' : H(\mathcal{H}) \to \mathbb{R}^m$ with $\sup_{v\in H(\mathcal{H}),\|v\|\leqslant 1}\|(L - L')v\|_2 < \epsilon$, $L'|_{\mathcal{P}}$ is a smooth embedding.*

Proof. Let $K \subseteq H(\mathcal{H})$ be a compact set containing $\mathcal{P}$. Furthermore let $b : H(\mathcal{H}) \to H(\mathcal{H})$ be a smooth and compactly supported bump function which equals the identity on K. Then, the proof of 3.13 shows that there is an $\eta > 0$ such that for every smooth map $\psi : H(\mathcal{H}) \to \mathbb{R}^m$ with $\sup_{x\in K}\|\psi(x) - (L\circ b)(x)\|_2 < \epsilon$ and $\sup_{(x,v)\in TK,\|v\|\leqslant 1}\|\mathrm{d}\psi_x(v) - d(L\circ b)_x(v)\|_2 < \eta$, $\psi|_{\mathcal{P}}$ is a smooth embedding. But for ψ linear we find

$$\begin{aligned}&\sup_{(x,v)\in TK,\|v\|\leqslant 1}\|\mathrm{d}\psi_x(v) - d(L\circ b)_x(v)\|_2\\ &\quad= \sup_{(x,v)\in TK,\|v\|\leqslant 1}\|\psi(v) - L(v)\|_2\\ &\quad= \sup_{v\in H(\mathcal{H}),\|v\|\leqslant 1}\|\psi(v) - L(v)\|_2\end{aligned}$$

and

$$\begin{aligned}&\sup_{x\in K}\|\psi(x) - (L\circ b)(x)\|_2\\ &\quad\leqslant \sup_{x\in K}\|x\| \sup_{v\in H(\mathcal{H}),\|v\|\leqslant 1}\|\psi(v) - L(v)\|_2.\end{aligned}$$

Thus, the claim holds for $\epsilon := \eta/\sup_{x\in K}\|x\| > 0$. □

A.5. Proof of proposition 4.6

In order to prove 4.6, let us first fix some notation. Let X be an oriented smooth compact manifold and $K(X)$ be the K-ring of X, i.e. the ring of equivalence classes of complex vector

bundles on X, where $E \sim E'$ if $E + n \simeq E' + m$ (an introductory text on this topic is e.g. [33])[12]. Let $p_i(X) \coloneqq p_i(TX) \in H^{2i}(X, \mathbb{Q})$ be the image of ith rational Pontryagin class evaluated on the tangent bundle TX. Furthermore, let $\hat{A}(p_1, \ldots, p_n)$ be the $\hat{A}$-genus, i.e. the genus associated to the power series $\frac{\sqrt{z}/2}{\sinh(\sqrt{z}/2)}$[34][13]. Let ch: $K(X) \to H^*(X, \mathbb{Q})$ be the Chern class and let $\mathrm{ch}(X) \coloneqq \mathrm{ch}(K(X)) \subseteq H^*(X, \mathbb{Q})$. For $z \coloneqq \sum_{i=0}^{\infty} z^{2i} \in H^*(X, \mathbb{Q})$, with $z_{2j} \in H^{2i}(X, \mathbb{Q})$, let $z^{(t)} \coloneqq \sum_{i=0}^{\infty} z^{2i} t^j$ for $t \in \mathbb{Q}$. Note that $(yz)^{(t)} = y^{(t)} z^{(t)}$.

For $z \in \mathrm{ch}(X)$, $d \in H^2(X, \mathbb{Q})$, $t \in \mathbb{Q}$ we define the Hilbert polynomial in t to be $H_{X,z,d}(t) \coloneqq (z^t e^{d/2} \hat{A}(p(X)))[X]$, where $[X]$ is the fundamental class of X [35, 36]. Furthermore for $q \in \mathbb{Q}$ let $\nu_2(q) \coloneqq$ exponent of 2 as primefactor of q. The result of Walgenbach in [21] is based on the result of Mayer in [37].

Theorem A.3. *[37] Let* X *be a* $2n$*-dimensional compact oriented smooth manifold and* H *be the Hilbert polynomial associated with* $d \in H^2(X; Z)$ *and* $z \in \mathrm{ch}(X)$.

Then X *cannot be immersed in Euclidean space of dimension* $-2\nu_2(H(\frac{1}{2})) - 1$ *and cannot be embedded in Euclidean space of dimension* $-2\nu_2(H(\frac{1}{2}))$.

Walgenbach obtains his results by computing $H(\frac{1}{2})$ for some $d \in H^2(X; Z)$ and $z \in \mathrm{ch}(X)$ using combinatorical methods. With the following lemma, 4.6 follows directly by observing that $\nu_2(a \cdot b) = \nu_2(a) + \nu_2(b)$. Let X_1, X_2 be $2n$-dimensional compact oriented smooth manifolds and let $\pi_i : X_1 \times X_2 \to X_i$, $i = 1, 2$, be the canonical projections.

Lemma A.4. *For* $z_i \in \mathrm{ch}(X_i)$, $d_i \in H^2(X_i, \mathbb{Q})$ *and* $[X_i] = (\pi_i)_*[X_1 \times X_2]$, $i = 1, 2$, *let* $z \coloneqq \pi_1^*(z_1)\pi_2^*(z_2)$, $d \coloneqq \pi_1^*(d_1) + \pi_2^*(d_2)$. *Then*

$$H_{X_1 \times X_2, z, d}(t) = H_{X_1, z_1, d_1}(t) H_{X_2, z_2, d_2}(t).$$

Proof. First, note that $z \in K(X_1 \times X_2)$, since

$$\begin{aligned}\pi_1^*(z_1)\pi_2^*(z_2) &= \pi_1^*\big(\mathrm{ch}(E_1)\big)\pi_2^*\big(\mathrm{ch}(E_2)\big) \\ &= \mathrm{ch}\big(\pi_1^*(E_1)\big)\mathrm{ch}\big(\pi_2^*(E_2)\big) = \mathrm{ch}\big(\pi_1^*(E_1) \oplus \pi_2^*(E_2)\big).\end{aligned}$$

Furthermore note that

$$\begin{aligned}p\big(X_1 \times X_2\big) &= p\big(T(X_1 \times X_2)\big) = p\big(\pi_1^* TX_1 \oplus \pi_2^* TX_2\big)\big) \\ &= p\big(\pi_1^*(TX_1)\big)p\big(\pi_2^*(TX_2)\big) = \pi_1^*\big(p(TX_1)\big)\pi_2^*\big(p(TX_2)\big).\end{aligned}$$

This, together with the fact that all cohomology classes involved are even dimensional and hence commute, yields

[12] Here m denotes the m-dimensional trivial bundle.

[13] This means that by construction the identitiy $p(E \oplus F) = p(E)p(F)$ of the total rational Pontryagin class transfers to the $\hat{A}$-genus.

$$
\begin{aligned}
H_{X_1\times X_2,z,d}(t) &= \left(z^{(t)}e^{d/2}\hat{A}\left(X_1\times X_2\right)\right)\left[X_1\times X_2\right]\\
&= \left(\pi_1^*(z_1)^{(t)}\pi_2^*(z_2)^{(t)}e^{\pi_1^*(d_1/2)+\pi_2^*(d_2/2)}\pi_1^*\left(\hat{A}\left(TX_1\right)\right)\pi_2^*\left(\hat{A}\left(TX_2\right)\right)\right)\left[X_1\times X_2\right]\\
&= \left(\pi_1^*\left(z_1^{(t)}e^{\pi_1^*(d_1)/2)}\hat{A}\left(X_1\right)\right)\pi_2^*\left(z_2^{(t)}e^{\pi_2^*(d_2)/2)}\hat{A}\left(X_2\right)\right)\right)\left[X_1\times X_2\right]\\
&= \left(z_1^{(t)}e^{\pi_1^*(d_1)/2)}\hat{A}\left(X_1\right)\right)\left[X_1\right]\left(z_2^{(t)}e^{\pi_2^*(d_2)/2)}\hat{A}\left(X_2\right)\right)\left[X_2\right]\\
&= H_{X_1,z_1,d_1}(t)H_{X_2,z_2,d_2}(t).
\end{aligned}
$$

□

A.6. Proof of proposition 4.8

Let X be a smooth compact n-manifold with tangent bundle TX. Let $\phi : X \to \mathbb{R}^{n+k}$ be an immersion and let NX be the normal bundle, i.e. $TX \oplus NX \simeq n + k$. Furthermore let ω be the total Stiefel–Whitney class. Let us state the following well-known result.

Proposition A.5. *[25] Let* i *be the degree of* $\overline{\omega}(X) = \omega(NX) \in H^*(X, \mathbb{Z}_2)$. *Then* X *cannot be immersed in Euclidean space of dimension* $n + i$ *and cannot be embedded in Euclidean space of dimension* $n + i + 1$.

In order to use this result, we need to compute $\overline{\omega}(PW_{n,k})$. The following is similar to [24], where the dual Stiefel–Whitney class of the real projective Stiefel manifolds is computed. Let L be the complex line bundle associated to the $U(1)$-principal bundle $W_{n,k} \to PW_{n,k}$ and let x be the mod 2 Euler class of L[14]. In [38], the cohomology ring $H^*(PW_{n,k}, \mathbb{Z}_2)$ for $k < n$ is found to be

$$\mathbb{Z}_2[x]\Big/\left(x^N\right) \oplus \Lambda(y_{n-k+1},\ldots,y_n),$$

with $y_i \in H^{2i-1}(PW_{n,k}, \mathbb{Z}_2)$. It is shown in [27], that $TPW_{n,k}$ is stably isomorphic to nkL^*, where L^* is regarded as a real vector bundle. Hence $\omega(TPW_{n,k}) = \omega(L^*)^{nk}$ and we obtain

$$\omega\left(NPW_{n,k}\right) = \overline{\omega}\left(TPW_{n,k}\right) = \omega\left(L^*\right)^{-nk}.$$

Since the odd Stiefel–Whitney classes of complex vector bundles (regarded as real vector bundles) vanish [33], and the Euler class is mapped to the top Stiefel-Whitney class under the coefficient homomorphism $H^*(PW_{n,k}, \mathbb{Z}) \to H^*(PW_{n,k}, \mathbb{Z}_2)$ [33], we get $\omega(L) = \omega(L^*) = 1 + x$. Thus

$$
\begin{aligned}
\omega\left(NPW_{n,k}\right) &= (1+x)^{-nk}\\
&= \sum_{i=1}^{\infty}(-1)^j\begin{pmatrix} nk+j-1 \\ j \end{pmatrix}x^j.
\end{aligned}
$$

We now want to find

$\gamma(m, k)$ = the biggest j such that the coefficient of x^j does not vanish in $\mathbb{Z}_2[x]/(x^N)$.

[14] I.e. the image of the Euler class of L under the coefficient homomorphism $H^*(PW_{n,k}, \mathbb{Z}) \to H^*(PW_{n,k}, \mathbb{Z}_2)$.

Since we factor over the ideal generated by x^N, we clearly have $j \leqslant N(n, k)$. Passing to mod 2, we get $2\gamma(m, k) = \sigma(n, k)$. This proves 4.8.

References

[1] Häffner H *et al* 2005 Scalable multiparticle entanglement of trapped ions *Nature* **438** 643–6
[2] Heinosaari T, Mazzarella L and Wolf M M 2013 Quantum tomography under prior information *Commun. Math. Phys.* **318** 355–74
[3] Weigert S 1992 Pauli problem for a spin of arbitrary length: a simple method to determine its wave function *Phys. Rev.* A **45** 7688
[4] Amiet J-P and Weigert S 1999 Reconstructing the density matrix of a spin s through Stern–Gerlach measurements: II. *J. Phys. A: Math. Gen.* **32** L269
[5] Amiet J-P and Weigert S 1998 Reconstructing the density matrix of a spin s through Stern–Gerlach measurements *J. Phys. A: Math. Gen.* **31** L543
[6] Finkelstein J 2004 Pure-state informationally complete and 'really' complete measurements *Phys. Rev.* A **70** 052107
[7] Mondragon V V D 2013 Determination of all pure quantum states from a minimal number of observables arXiv:1306.1214
[8] Carmeli C, Heinosaari T, Schultz J and Toigo A 2014 Tasks and premises in quantum state determination *J. Phys. A: Math. Theor.* **47** 075302
[9] Carmeli C, Heinosaari T, Schultz J and Toigo A 2015 Expanding the principle of local distinguishability *Phys. Rev.* A **91** 042121
[10] Flammia S T, Silberfarb A and Caves C M 2005 Minimal informationally complete measurements for pure states *Found. Phys.* **35** 1985–2006
[11] Gross D 2011 Recovering low-rank matrices from few coefficients in any basis *IEEE Trans. Inf. Theory* **57** 1548–66
[12] Flammia S T, Gross D, Liu Y-K and Eisert J 2012 Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators *New J. Phys.* **14** 095022
[13] Millane R 1990 Phase retrieval in crystallography and optics *J. Opt. Soc. Am.* A **7** 394–411
[14] Gross D, Krahmer F and Kueng R 2015 A partial derandomization of phaselift using spherical designs *J. Fourier Anal. Appl.* **21** 229–66
[15] Gross D, Liu Y-K, Flammia S T, Becker S and Eisert J 2010 Quantum state tomography via compressed sensing *Phys. Rev. Lett.* **105** 150401
[16] Johnston N and Gutoski G 2014 Process tomography for unitary quantum channels *J. Math. Phys.* **55** 032201
[17] Charles I H D, Baldwin H and Kalev A 2014 Quantum process tomography of unitary and near-unitary maps *Phys. Rev.* A **90** 012110
[18] Holevo A S 2011 *Probabilistic and Statistical Aspects of Quantum Theory* vol 1 (Berlin: Springer)
[19] Busch P, Grabowski M and Lahti P J 1995 *Operational Quantum Physics* vol 31 (Berlin: Springer)
[20] Warner F W 1971 *Foundations of Differentiable Manifolds and Lie Groups* vol 94 (Berlin: Springer)
[21] Walgenbach M 2001 Lower bounds for the immersion dimension of homogeneous spaces *Topology Appl.* **112** 71–86
[22] Cubitt T, Montanaro A and Winter A 2008 On the dimension of subspaces with bounded Schmidt rank *J. Math. Phys.* **49** 022107
[23] Davidson K R 1996 *C*-algebras by Example* vol 6 (Providence, RI: AMS)
[24] Barufatti N E 1994 Obstructions to immersions of projective stiefel manifolds *Contemp. Math.* **161** 281–287
[25] Milnor J W and Stasheff J D 1974 *Characteristic Classes* vol 93 (Princeton, NJ: Princeton University Press)
[26] Milgram R J 1967 Immersing projective spaces *Ann. Math.* **85** 473–82
[27] Astey L, Gitler S, Micha E and Pastor G 2000 Parallelizability of complex projective stiefel manifolds *Proc. Am. Math. Soc.* **128** 1527–30 (www.jstor.org/stable/119668)
[28] Hirsch M W 1959 Immersions of manifolds *Trans. Am. Math. Soc.* **93** 242–76
[29] Atiyah M F 1962 Immersions and embeddings of manifolds *Topology* **1** 125–32
[30] Rees E 1971 Some embeddings of lie groups in euclidean space *Mathematika* **18** 152–6

[31] Hirsch M W 1976 *Differential Topology* (Berlin: Springer)
[32] Bagby T, Bos L and Levenberg N 2002 Multivariate simultaneous approximation *Constructive Approx.* **18** 569–77
[33] Hatcher A 2003 *Vector Bundles and K-Theory* http://math.cornell.edu/~hatcher/VBKT/VBpage.html
[34] Hirzebruch F 1995 *Topological Methods in Algebraic Geometry* vol 131 (Berlin: Springer)
[35] Borel A and Hirzebruch F 1959 Characteristic classes and homogeneous spaces: II. *Am. J. Math.* **81** 315–82
[36] Atiyah M F and Hirzebruch F 1959 Quelques théorèmes de non-plongement pour les variétés différentiables *Bulletin de la Société Mathématique de France* **87** 383–96
[37] Mayer K H 1965 Elliptische differentialoperatoren und ganzzahligkeitssätze für charakteristische zahlen *Topology* **4** 295–313
[38] Astey L, Gitler S, Micha E and Pastor G 1999 Cohomology of complex projective stiefel manifolds *Can. J. Math.* **51** 897–914

Subject: Re: Permission to include article (DOI:10.1088/1751-8113/48/26/265303) in my dissertation
From: Permissions <permissions@iop.org>
Date: 22.07.2016 13:01
To: Michael Kech <kech@ma.tum.de>

Dear Michael Kech,

Thank you for your email and for taking the time to seek this permission.

Regarding:

Michael Kech et al 2015 J. Phys. A: Math. Theor. 48 265303

When you transferred the copyright in your article to IOP, we granted back to you certain rights, including the right to include the Accepted Manuscript of the article within any thesis or dissertation. Please note you may need to obtain separate permission for any third party content you included within your article.

Please include citation details, "© IOP Publishing. Reproduced with permission. All rights reserved" and for online use, a link to the Version of Record.

The only restriction is that if, at a later date, your thesis were to be published commercially, further permission would be required.

Please let me know if you have any further questions.

In the meantime, I wish you the best of luck with the completion of your dissertation.

Kind regards,

Kathryn Shaw

Copyright & Permissions Team
Gemma Alaway – Rights & Permissions Adviser
Kathryn Shaw - Editorial Assistant

Contact Details
E-mail: permissions@iop.org

For further information: http://iopscience.iop.org/page/copyright

Please see our Author Rights Policy http://ioppublishing.org/author-rights/

Please note: We do not provide signed permission forms as a separate attachment. Please print this email and provide it to your institution as proof of permission.

Please note: Any statements made by IOP Publishing to the effect that authors do not need to get

permission to use any content are not intended to constitute any sort of legal advice. Authors must make their own decisions as to the suitability of the content they are using and whether they require permission for it to be published within their article.

From: Michael Kech <kech@ma.tum.de>
To: permissions@iop.org,
Date: 21/07/2016 12:44
Subject: Permission to include article (DOI:10.1088/1751-8113/48/26/265303) in my dissertation

---

Dear Sir or Madame,

I am currently preparing a cumulative dissertation. I am an author of the article

The Role of Topology in Quantum Tomography
by Michael Kech, Peter Vrana, Michael Wolf
published in Journal of Physics A: Mathematical and Theoretical, Volume 48, Number 26

and I would like to ask for permission to include this article in my dissertation.

Kind regards

Michael Kech

Constrained Quantum Tomography of Semi-Algebraic Sets with Applications to Low-Rank Matrix Recovery

M. Kech and M. Wolf August 24, 2016

Quantum state tomography is considered in the scenario where both the set of relevant quantum states and the set of admissible measurement schemes are constrained by algebraic equalities and inequalities. Upper bounds on the minimal number of von Neumann measurements needed to discriminate any two states of a given subset of the state space are provided.

Similar results are obtained if the tomography scheme consists of determining expectation values of local observables.

1 Main Result

Let $POVM_{\mathcal{H}}^{m}$ be the set of POVMs on $\mathcal{H}$ with m outcomes and let

$$POVM_{\mathcal{H}}^{1,m} := \{P \in POVM_{\mathcal{H}}^{m} | \, \forall i \in \{1,\dots,m\} : \operatorname{rank} P(\{i\}) = 1\} \subseteq POVM_{\mathcal{H}}^{m}$$

be the set of rank one POVMs with m outcomes. Furthermore, let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a subset and let $\Delta(\mathcal{R}) := \{\lambda(\varrho - \varrho') | \, \varrho, \varrho' \in \mathcal{R}, \lambda > 0\}$. A semi-algebraic subset $\mathcal{D} \subseteq H(\mathcal{H}) \setminus \{0\}$ is said to represent $\Delta(\mathcal{R})$ iff the following condition holds: If there exists a measurment scheme $M \in MS_{\mathcal{H}}$ such that $\operatorname{Ker} D_M \cap \Delta(\mathcal{R}) \setminus \{0\}$ is non-empty, then so is $\operatorname{Ker} D_M \cap \mathcal{D}$.

Theorem 1 (Universality)**.** *Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a subset and let $\mathcal{D} \subseteq H(\mathcal{H})$ be a semi-algebraic subset that represents $\Delta(\mathcal{R})$. If $k(m-1) > \dim \mathcal{D}$, then almost all measurement schemes $M \in \prod_{i=1}^{k} POVM_{\mathcal{H}}^{1,m}$ are stably $\mathcal{R}$-complete.*

The proof of this theorem is inspired by the approach taken in [1]. In principle, the argument is close to the proof of the Whitney embedding theorem given in Chapter 2 of the present dissertation. Proving that the dimension argument remains valid when restricting to rank one POVMs is the main technical step and strongly relies on the dimension theory of real algebraic geometry. Naturally, from this result one can straightforwardly prove a Whitney type embedding result.

Corollary 2 (Whitney)**.** *Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a semi-algebraic subset. If $k(m-1) > 2 \dim \mathcal{R}$, then almost all measurement schemes $M \in \prod_{i=1}^{k} POVM_{\mathcal{H}}^{1,m}$ are stably $\mathcal{R}$-complete.*

2 Application

Theorem 1 can be straightforwardly applied to quantum states of bounded rank and yields the following result:

Theorem 3 (States of rank at most r)**.** *If $k(m-1) > 4r(n-r)$, then almost all measurement schemes $M \in \prod_{i=1}^{k} POVM_{\mathcal{H}}^{1,m}$ are stably $\mathcal{S}_r(\mathcal{H})$-complete.*

The following special case of this result might be of particular interest.

Corollary 4 (States of rank at most r)**.** *If $k(n-1) > 4r(n-r)$, then almost all collections of k von Neumann measurements $M \in \prod_{i=1}^{k} POVM_{\mathcal{H}}^{1,n}$ are stably $\mathcal{S}_r(\mathcal{H})$-complete.*

For $r = 1$ this reproduces the main result of [2]. Corollary 4 yields an upper bound on the minimal number of von Neumann measurements needed to discriminate any two quantum states of rank at most r and the non-immersion results of [3] show that this bound is indeed tight for dimensions greater than four.

3 Legal statement

The project was assigned by Prof. Michael Wolf. I am the principal author of this article and I was significantly involved in all parts of this article.

References

[1] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Applied and Computational Harmonic Analysis*, 20(3):345–356, 2006.

[2] Damien Mondragon and Vladislav Voroninski. Determination of all pure quantum states from a minimal number of observables. *arXiv preprint arXiv:1306.1214*, 2013.

[3] Markus Walgenbach. Lower bounds for the immersion dimension of homogeneous spaces. *Topology and its Applications*, 112(1):71–86, 2001.

Constrained Quantum Tomography of Semi-Algebraic Sets with Applications to Low-Rank Matrix Recovery

Michael Kech[1,*] and Michael M. Wolf[1,†]

[1] *Department of Mathematics, Technische Universität München, 85748 Garching, Germany*

(Dated: August 11, 2016)

We analyse quantum state tomography in scenarios where measurements and states are both constrained. States are assumed to live in a semi-algebraic subset of state space and measurements are supposed to be rank-one POVMs, possibly with additional constraints. Specifically, we consider sets of von Neumann measurements and sets of local observables. We provide upper bounds on the minimal number of measurement settings or outcomes that are required for discriminating all states within the given set. The bounds exploit tools from real algebraic geometry and lead to generic results that do not only show the existence of good measurements but guarantee that almost all measurements with the same dimension characteristic perform equally well.

In particular, we show that on an n-dimensional Hilbert space any two states of a semi-algebraic subset can be discriminated by k generic von Neumann measurements if $k(n-1)$ is larger than twice the dimension of the subset. In case the subset is given by states of rank at most r, we show that k generic von Neumann measurements suffice to discriminate any two states provided that $k(n-1) > 4r(n-r) - 2$. We obtain corresponding results for low-rank matrix recovery of hermitian matrices in the scenario where the linear measurement mapping is induced by tight frames.

Keywords: quantum tomography, semi-algebraic sets, low-rank matrix recovery

Contents

*Electronic address: kech@ma.tum.de
†Electronic address: wolf@ma.tum.de

I. INTRODUCTION

Let us note in the beginning that the reader mainly interested in low-rank matrix recovery can find our corresponding results in Section IV. There we find linear measurement mappings induced by tight frames that can discriminate any two matrices of rank at most r.

Quantum state tomography, which aims at identifying quantum states from the outcomes of an experiment, is a central task in quantum information science. Full state tomography is often challenging and sometimes infeasible. However, if there is some prior information about the state under investigation, this can considerably simplify the problem: the number of measurement settings necessary to uniquely identify a given state can significantly decrease if the state is not arbitrary but is known to lie on a confined subset of state space.

Using topological properties of the measurement map and the constrained set, lower bounds on the minimal number of measurement settings necessary to discriminate any two pure states were obtained in [1]. Relating these topological features of the measurement map to stability properties, it was shown in [2] that under the premise of stability the approach of [1] can be generally applied. Using this result, lower bounds on the necessary number of measurement settings for several other subsets were obtained in [2].

The present paper deals with the issue of finding upper bounds: given a subset of state space, find a measurement scheme that can discriminate any two states of this subset with as few measurement settings as possible. This appears to be a rather hard problem in general. Already in the case of pure state quantum tomography it has received significant attention in topology [3, 4], quantum information science [1, 5–9, 9–14] and sampling theory [15–18].

In addition to constraining the set of states, we also restrict the set of measurements in order to capture the fact that arbitrary measurements may not be feasible in an experiment. The imposed constraints could for example be the restriction to von Neumann measurements or to local measurements when dealing with a multipartite system. The case of pure state tomography with von Neumann measurements was addressed in [11, 19, 20]. In [11, 19] it was shown that any two pure states can be discriminated by merely 4 von

Neumann measurements. This is known to be sharp for pure states of an n-dimensional Hilbert space if $n > 4$ and [20] has a special focus on the cases $n \leq 4$. The more general setting of low-rank matrix recovery with restricted measurements was considered in [21]. However, their focus is to determine the asymptotic behaviour, and this allows us to improve on some of their results.

We propose a method that can deal with these problems rather generally and we then apply it to different scenarios.

In this paper we neither consider the statistical aspects of quantum tomography nor the algorithmic problem of reconstructing the state from the measurement data.

Outline. In Section II we fix notation, introduce measurement schemes that are relevant in the following and give some preliminary results about hermitian matrices of bounded rank. Furthermore, we illustrate the connection between phase retrieval and quantum tomography.

In Section III, we propose a method to find sets of measurements that can discriminate any two states of a given subset of the state space, generalizing the approach taken in [15] to find frames for the phase retrieval problem. The method can be applied to all semi-algebraic subsets and it can naturally deal with constrained measurement like e.g. von Neumann measurements. Rather than giving explicit constructions, the method asserts that almost all sets of measurement that fulfil certain constraints allow for a unique identification.

In Section IV, we apply this procedure to low-rank matrix recovery, showing that a generic frame with $m > 4r(n-r)$ frame vectors can discriminate any two hermitian matrices of rank at most r. This generalizes [16] where the case $r = 1$ was considered. In addition we shown that the statement also holds when restricting to tight frames.

In Section V, we prove that under a further condition the sets of measurements obtained by the method introduced in Section III fulfil the stability property introduced in [2]. In the scenarios where the method is feasible this condition is satisfied and therefore the stability property holds rather generally.

In Section VI, we present the main result of this paper. Loosely speaking, it asserts that one can perform tomography on all semi-algebraic subsets of the state space by measuring sets of positive operator valued measures that consist exclusively of rank one operators, in particular von Neumann measurements. From this result we straightforwardly obtain Whitney type embedding results for these measurement schemes. Furthermore, we consider the problem of discriminating states of bounded rank: In [1, 2] lower bounds on the number of measurement outcomes necessary to uniquely identify quantum states with bounded rank were established and these lower bounds turned out to be close to the upper bounds obtained in [1] where it was shown that $4r(n-r)$ measurement outcomes suffice in order to identify states of an n-dimensional system with rank at most r. However, the measurement that does realize this upper bound has a rather complicated structure. We prove that the same upper bounds as in [1] can be realized when measuring a positive operator valued measure which exclusively consist of rank one operators and we prove similar results for measuring sets of von Neumann measurements. Note that our results come with less measurement outcomes than the compressed sensing approach of [10], however we do not provide a tractable reconstruction procedure.

Section VII deals with the problem of reconstructing states of multipartite systems from

the expectation values of local observables. Just like in Section V, we first give a theorem stating that one can do tomography on all semi-algebraic subsets of the state-space by performing measurements of this type. Then we obtain Whitney type embedding results and also for the problem of identifying states of bounded rank we obtain corresponding results.

In Section VIII, proofs of technical results are given.

Most of our results assert that almost all measurements have a certain property. In the appendix we present the measure with respect to which this is true.

II. PRELIMINARIES

Throughout $\mathcal{H}$ denotes a finite-dimensional complex Hilbert space. $H(\mathcal{H})$ denotes the real vector space of hermitian operators[1] on $\mathcal{H}$ and $\mathcal{S}(\mathcal{H})$ denotes the set of quantum states on $\mathcal{H}$, i.e. $\mathcal{S}(\mathcal{H}) = \{\varrho \in H(\mathcal{H}) : \varrho \geq 0, \mathrm{tr}(\varrho) = 1\}$. We regard $H(\mathcal{H})$ as an inner product space, equipping it with the Hilbert-Schmidt inner product. The Hilbert Schmidt norm is denoted by $\|\cdot\|_2$. By $SH(\mathcal{H}) := \{X \in H(\mathcal{H}) : \ \|X\|_2^2 = \mathrm{tr}(X^2) = 1\}$ we denote the unit sphere in $H(\mathcal{H})$. Furthermore, for a subset $A \subseteq H(\mathcal{H})$, $\Delta(A)$ denotes the set of differences of operators in A, i.e. $\Delta(A) = \{X - Y : X, Y \in A\}$. $M(m, n, \mathbb{C})$ $(M(m, n, \mathbb{R}))$ denotes the set of complex (real) $m \times n$ matrices and we write $M(n, \mathbb{C})$ $(M(n, \mathbb{R}))$ as shorthand for $M(n, n, \mathbb{C})$ $(M(n, n, \mathbb{R}))$.

In the following, measurements are modelled by linear mappings form the set of hermitian operators (respectively hermitian matrices) to $\mathbb{R}^m$, where m is the number of measurement outcomes.

Definition II.1. *(Measurement map.) A linear mapping $h : H(\mathcal{H}) \to \mathbb{R}^m$ is called a measurement map. The number of outcomes of h is m.*

(Constrained) Measurements in Quantum Mechanics

In this section we focus on the specific measurement maps that typically arise in quantum mechanics. In quantum mechanics positive operator valued measures (POVMs) are used to describe general measurements [22, 23]. For the purpose of this paper a POVM on $\mathcal{H}$ is a tuple $P = (Q_1, ..., Q_m)$ of positive semidefinite operators on $\mathcal{H}$ such that

$$\sum_{i=1}^{m} Q_i = \mathbb{1}_{\mathcal{H}}.$$

An element of P is called an effect operator. We define the dimension of P by $\dim P := |P|$.

A whole measurement scheme might consist of measuring more than one POVM.

Definition II.2. *A measurement scheme on $\mathcal{H}$ is a tuple $M = (P_1, ..., P_k)$ of POVMs on $\mathcal{H}$. We define the dimension of M by* $\dim M := \dim P_1 + ... + \dim P_k$.

[1] We denote the adjoint of a linear operator $B : \mathcal{H}_1 \to \mathcal{H}_2$ by $B^\dagger$.

A POVM P can be identified with the measurement scheme that just contains P. In the following we sometimes make use of this identification and regard POVMs as measurement schemes.

A POVM $P = (Q_1, ..., Q_m)$ induces a measurement map

$$\begin{aligned} h_P : H(\mathcal{H}) &\to \mathbb{R}^m \\ X &\mapsto \big(\mathrm{tr}(Q_1 X), ..., \mathrm{tr}(Q_m X)\big). \end{aligned}$$

Similarly a measurement scheme $M = (P_1, ..., P_k)$ induces a measurement map

$$\begin{aligned} h_M : H(\mathcal{H}) &\to \mathbb{R}^{|P_1|+...+|P_k|} \\ X &\mapsto \big(h_{P_1}(X), ..., h_{P_k}(X)\big). \end{aligned}$$

Definition II.3. *A measurement scheme M is called $\mathcal{R}$-complete for a subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ if $h_M|_{\mathcal{R}}$ is injective.*

Our main results are statements about rank one POVMs and von Neumann measurements, so let us define these terms: A POVM P is called rank one POVM if all effect operators are of rank one. We denote the set of m-dimensional rank one POVMs on $\mathcal{H}$ by $\mathcal{M}_1^m(\mathcal{H})$. In the following we implicitly assume that $m \geq \dim \mathcal{H}$ because otherwise $\mathcal{M}_1^m(\mathcal{H})$ would be empty.

Later on we often use the following correspondence between linear isometries and $\mathcal{M}_1^m(\mathbb{C}^n)$: The equations

$$M^\dagger M = \mathbb{1}_n, \ M \in M(m, n, \mathbb{C}),$$

can be considered as real algebraic equations under the identification $M(m, n, \mathbb{C}) \simeq \mathbb{R}^{2nm}$. The solution set $U(m, n)$ is the set of linear isometries $U : \mathbb{C}^n \to \mathbb{C}^m$. Note that $U(m, n)$ is non-empty if and only if $m \geq n$ and that for $n = m$ it is the set of unitaries. We write $U(n)$ as shorthand for $U(n, n)$.

Let $\{e_i\}_{i\in\{1,...,m\}}$ be the standard basis of $\mathbb{C}^m$. Then, the sought correspondence is given by the map

$$\begin{aligned} \phi : U(m, n) &\to \mathcal{M}_1^m(\mathbb{C}^n) \\ U &\mapsto (U^\dagger e_1 e_1^\dagger U, ..., U^\dagger e_1 e_1^\dagger U). \end{aligned} \tag{1}$$

If the effect operators of a POVM are projections on mutually orthogonal subspaces, the POVM is called von Neumann measurement. In this paper, we just deal with rank one von Neumann measurements and therefore, in the following, the term von Neumann measurement always refers to rank one von Neumann measurements. Note, that the set of rank one von Neumann measurements is precisely the set of $(\dim \mathcal{H})$-dimensional rank one POVMs.

The measurement scheme consisting of k m-dimensional rank one POVMs on $\mathcal{H}$ is denoted by $\mathcal{M}_{1,k}^m(\mathcal{H})$, i.e.

$$\mathcal{M}_{1,k}^m(\mathcal{H}) = \{(P^1, ..., P^k) : P^i \in \mathcal{M}_1^m(\mathcal{H})\}.$$

For $m = \dim \mathcal{H}$ this is the set of k rank one von Neumann measurements which, we denote by $\mathcal{M}_{\mathrm{vN}}^k(\mathcal{H})$.

Hermitian Matrices of Bounded Rank

In this section we prove a lemma about hermitian operators with bounded rank, which is frequently used in the following. Denote by $\mathcal{P}_r(\mathcal{H})$ the set of hermitian operators on $\mathcal{H}$ with rank at most r, i.e. $\mathcal{P}_r(\mathcal{H}) := \{X \in H(\mathcal{H}) : \mathrm{rank}(X) \leq r\}$. We write $\mathcal{P}_r^n$ as shorthand for $\mathcal{P}_r(\mathbb{C}^n)$.

Lemma II.1. *$\mathcal{P}_r^n$ is a real algebraic set of dimension $r(2n-r)$.*

Proof. First note that $\mathcal{P}_r^n$ is a real algebraic set: It is given by the set of points $X \in M(n,\mathbb{C})$ for which all $(r+1)\times(r+1)$-minors vanish and that satisfy $X = X^\dagger$. These conditions turn into a set of real algebraic equations under the canonical identification $M(n,\mathbb{C}) \simeq \mathbb{R}^{2n^2}$.

To determine the dimension of $\mathcal{P}_r^n$ consider the semi-algebraic set $V_r^n = \{(P_1,...,P_r) : P_i \in \mathcal{P}_1^n,\ \mathrm{tr}(P_iP_j) = \delta_{ij},\ P_i \geq 0\}$ [2]. The dimension of V_r^n is given by $r(2n-r)-r$. To see this, consider the smooth and transitive action of $U(n)$ on the complex matrices $M(n,\mathbb{C})$ given by $(U,M) \to (U, UMU^\dagger)$ and let V_D be the orbit of the diagonal matrix $D := \mathrm{diag}(r, r-1, ..., 1, 0, ...)$ under this action. Noting that the stabilizer subgroup of D is $U(n-r)\times U(1)^r$ we obtain $V_D \simeq U(n)/(U(n-r)\times U(1)^r)$ by Theorem 3.62 of [24]. But the semi-algebraic map $\psi : V_r^n \to V_D,\ (P_1,...,P_r) \mapsto \sum_{j=1}^r jP_j$ is clearly bijective. Hence we find $\dim V_r^n = \dim(U(n)/(U(n-r)\times U(1)^r)) = n^2 - (n-r)^2 - r = r(2n-r) - r$ by Theorem 2.8.8 and Proposition 2.8.14 of [25].

The semi-algebraic map

$$\begin{aligned} \eta : \mathbb{R}^r \times V_r^n &\to \mathcal{P}_r^n \\ (\lambda_1,...,\lambda_r, P_1,...,P_r) &\mapsto \sum_{i=1}^r \lambda_i P_i. \end{aligned} \tag{2}$$

is clearly surjective. By Theorem 2.8.8 of [25], we hence conclude that $\dim \mathcal{P}_r^n \leq \dim V_r^n + r = r(2n-r)$ and furthermore that indeed $\dim \mathcal{P}_r^n = r(2n-r)$ by noting that ϕ is injective if we require $\lambda_1 > ... > \lambda_r > 0$. □

Corollary II.2. *The set $\mathcal{D}_1 := \{X \in \mathcal{P}_r^n :\ tr(X^2) = 2\}$ is a real algebraic set of dimension $r(2n-r)-1$ and the set $\mathcal{D}_2 := \{X \in \mathcal{P}_r^n :\ tr(X^2) = 2,\ tr(X) = 0\}$ is a real algebraic set of dimension $r(2n-r)-2$.*

Proof. From the proof of Lemma II.1 it is immediate that both $\mathcal{D}_1$ and $\mathcal{D}_2$ are real algebraic sets. To determine the dimension of $\mathcal{D}_1$, one can go along the lines of the proof of Lemma II.1 and simply replace $\mathbb{R}^n$ by the unit sphere S^{n-1} in the definition of the mapping η. Similarly, to determine the dimension $\mathcal{D}_2$, one can go along the lines of the proof of Lemma II.1 and this time replace $\mathbb{R}^n$ by $\{x \in S^{n-1} : \sum_{i=1}^n x_i = 0\}$ in the definition of the mapping η. □

[2] A hermitian matrix is positive semidefinite if and only if all of its principal minors are greater than of equal to zero. Thus, the equations $P_i \geq 0$ can be regarded as algebraic inequalities.

Frames and Rank One POVMs

Finally, we discuss the connection between pure state tomography and the phase retrieval problem in sampling theory. A finite set $F = \{v_1, ..., v_m\}$ of vectors in $\mathbb{C}^n$ is called a frame if there exist constants $a, b > 0$ such that

$$a\|x\|_2^2 \leq \sum_{i=1}^{m} |\langle x, v_i\rangle|^2 \leq b\|x\|_2^2 \text{ for all } x \in \mathbb{C}^n. \tag{3}$$

A frame $F = \{v_1, ..., v_m\}$ induces a measurement map

$$\begin{aligned} M_F : \mathbb{C}^n/\sim &\to \mathbb{R}^m \\ [x] &\mapsto (|\langle v_1, x\rangle|^2, ..., |\langle v_m, x\rangle|^2) \end{aligned}$$

where $x \sim y$ iff there is a $\lambda \in \mathbb{R}$ such that $x = e^{i\lambda}y$ [3]. Since the task in phase retrieval is to reconstruct signals modulo phase from intensity measurements, one considers frames F such that M_F is injective.

Each frame $F = \{v_1, ..., v_m\}$ induces a map

$$\begin{aligned} h_F : H(\mathbb{C}^n) &\to \mathbb{R}^m \\ X &\to (\mathrm{tr}(Xv_1v_1^\dagger), ..., \mathrm{tr}(Xv_mv_m^\dagger)). \end{aligned} \tag{4}$$

Noting that $h_F(xx^\dagger) = M_F(x)$, we conclude that $h_{P_F}|_{\mathcal{P}_1^n}$ is injective if and only if M_F is injective.

A corollary of one of our main results is a statement about tight frames, so let us define this term. A frame F is called tight frame if $a = b$ in inequality (3). If in addition $a = b = 1$, F is called tight frame.

The following proposition shows the well-know fact that tight frames correspond to rank one POVMs.

Proposition II.3. *Let F be a tight frame. Then the associated set of rank one operators P_F is a POVM.*

Proof. Let $F = \{v_1, ..., v_m\}$. Since F is a tight frame, we obtain the following equality from inequality (3):

$$\sum_{i=1}^{m} |\langle v_i, x\rangle|^2 = \|x\|_2^2.$$

This can be rewritten as

$$\sum_{i=1}^{m} |\langle v_i, x\rangle|^2 = \mathrm{tr}(xx^\dagger \sum_{i=1}^{m} v_iv_i^\dagger) = \|x\|^2.$$

[3] Note that M_F is also well-defined for $F = \{v_1, ..., v_m\}$ with $v_i \in \mathbb{C}^n$, i.e. if we do not require F to be a frame.

But since this holds for all $x \in \mathbb{C}^n$ we conclude that $\sum_{i=1}^m v_i v_i^\dagger = \mathbb{1}_{\mathbb{C}^n}$: Assume $\sum_{i=1}^m v_i v_i^\dagger \neq \mathbb{1}_{\mathbb{C}^n}$. Since $\sum_{i=1}^m v_i v_i^\dagger$ is hermitian there has to be an eigenvector w of $\sum_{i=1}^m v_i v_i^\dagger$ with eigenvalue $\lambda \neq 1$. But then $w^\dagger \sum_{i=1}^m v_i v_i^\dagger w = \lambda \|w\|_2^2 \neq \|w\|_2^2$, a contradiction. □

Remark Note that the correspondence is given by the map ϕ defined in equation (1) where the frame vectors are given by the rows of the isometry.

Let P be a POVM. In pure state tomography, not $h_P|_{\mathcal{P}_1^n}$ is required to be injective, but $h_P|_{\mathcal{S}_1^n}$ where $\mathcal{S}_1^n := \{\varrho \in \mathcal{S}(\mathbb{C}^n) : \varrho^2 = \varrho\}$ is the set of pure states. However, by the definition of a POVM, $\mathbb{1}_n \in P$ and this implies that if $h_P|_{\mathcal{S}_1^n}$ is injective, also $h_P|_{\mathcal{P}_1^n}$ is injective. From this point of view, pure state quantum tomography with rank one POVMs is equivalent to phase retrieval with tight frames.

III. THE BASIC IDEA

Let us begin by explaining the basic idea of the method we utilize to find one-to-one measurement schemes which originates from the approach taken in [15] to find frames for the phase retrieval problem.

The method essentially relies on the following observation: A measurement scheme $P := ((Q_1^1, ..., Q_m^1), ..., (Q_1^k, ..., Q_m^k))$ is $\mathcal{R}$-complete with respect to a subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ if and only if the equations

$$\operatorname{tr}(Q_i^j X) = 0, \quad i \in \{1, ..., m-1\}, j \in \{1, ..., k\} \tag{5}$$

have no solution for $X \in \Delta(\mathcal{R}) - \{0\}$.

For a given subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$, we want to characterize non-injective measurement schemes via the equations (5) and use the dimension theory of semi-algebraic sets to show that these have measure zero. Therefore, we consider measurement schemes that are constrained by real algebraic equalities or inequalities. In the following, the set of measurement schemes is a semi-algebraic set $\mathcal{M}$ such that for all $M \in \mathcal{M}$ we have $\dim P = m, \forall P \in M$ and $|M| = k$ where $m, k \in \mathbb{N}$ are some fixed numbers. For example, if $k = 1$, this could be the restriction to the set of m-dimensional rank one POVMs $\mathcal{M}_1^m(\mathcal{H})$. Furthermore, in order to ensure that the equations (5) in fact become real algebraic equations, we have to replace $\Delta(\mathcal{R}) - \{0\}$ by a suitable semi-algebraic set. We do this by constructing a semi-algebraic set $\mathcal{D} \subseteq H(\mathcal{H})$[4] with the following property: If there is a measurement scheme M and an $X \in \Delta(\mathcal{R}) - \{0\}$ with

$$h_M(X) = 0 \tag{6}$$

then there exists $X' \in \mathcal{D}$ with

$$h_M(X') = 0. \tag{7}$$

[4] Here we identify $H(\mathcal{H})$ with $(\dim \mathcal{H})^2$-dimensional real affine space.

If a semi-algebraic set $\mathcal{D} \subseteq H(\mathcal{H})$ with $0 \notin \mathcal{D}$ has this property, we say that $\mathcal{D}$ represents $\Delta(\mathcal{R}) - \{0\}$.

The solution set of the equations (7) characterizes the non-injective measurement schemes: Let $\tilde{\mathcal{M}}$ be the real semi-algebraic set obtained from $\mathcal{M} \times \mathcal{D}$ by imposing the equations (7). By construction of $\mathcal{D}$, the non-injective measurement schemes are contained in the projection of $\tilde{\mathcal{M}} \subseteq \mathcal{M} \times \mathcal{D}$ on the first factor with the canonical projection $\pi_1 : \mathcal{M} \times \mathcal{D} \to \mathcal{M}$. But if $\dim \tilde{\mathcal{M}} < \dim \mathcal{M}$, we also have $\dim \pi_1(\tilde{\mathcal{M}}) < \dim \mathcal{M}$ [5] and thus the non-injective measurement schemes have measure zero in $\mathcal{M}$. Here we used the well-know fact that, for a suitably chosen measure, the measure of a semi-algebraic subset S of a semi-algebraic set A has measure zero in A if $\dim A > \dim S$. For more details on the measure see Appendix A.

This approach is most efficient if the equations (7) are transversal to $\mathcal{M} \times \mathcal{D}$. In this case $\dim \tilde{\mathcal{M}} < \dim \mathcal{M}$ is equivalent to $k(m-1) > \dim \mathcal{D}$ and thus the quality of our result is determined by how low-dimensional we can choose the semi-algebraic set $\mathcal{D}$.

IV. LOW-RANK MATRIX RECOVERY WITH FRAMES

To illustrate how this procedure works, let us consider the problem of low-rank matrix recovery with frames. We show that any two hermitian matrices of rank at most r can be discriminated from a generic frame with $m \geq 4r(n-r)$ frame vectors. The proof we give is inspired by the proof of Theorem 3.1 in [15]. Let $r \in \{1, \ldots, [n/2]\}$ [6].

Theorem IV.1. *(Low-Rank Matrix Recovery with Frames.) Let $m \geq 4r(n-r)$. For almost all frames $F = \{v_1, .., v_m\}$ the map $h_F|_{\mathcal{P}_r^n}$ is injective.*

Proof. Let $F = (v_1, ..., v_m)$, $v_i \in \mathbb{C}^n$, and consider the equations

$$v_i^\dagger X v_i = 0, \ i \in \{1, ..., m\}, \tag{8}$$

in $v_i \in \mathbb{C}^n$, $X \in \Delta(\mathcal{P}_r^n) - \{0\}$. As explained above, these equations determine the subset N of $F \in \mathbb{C}^{nm} \simeq \mathbb{R}^{2nm}$ for which $h_F|_{\mathcal{P}_r^n}$ fails to be injective.

Note that $\Delta(\mathcal{P}_r^n) - \{0\} = \mathcal{P}_{2r}^n - \{0\}$. Consider the algebraic set $\mathcal{D} := \{X \in \mathcal{P}_{2r}^n : \mathrm{tr}(X^2) = 1\}$ and note that we have $\dim \mathcal{D} = 4r(n-r) - 1$ by Corollary II.2. Furthermore, $\mathcal{D}$ represents $\Delta(\mathcal{P}_r^n) - \{0\}$: Clearly $0 \notin \mathcal{D}$. Next, consider a measurement scheme M and $X \in \mathcal{P}_{2r}^n - \{0\}$ such that $h_M(X) = 0$. But then there is $X' := \frac{X}{\|X\|_2} \in \mathcal{D}$ such that $h_M(X') = \frac{1}{\|X\|_2} h_M(X) = 0$.

Under the identification $\mathbb{C}^{nm} \simeq \mathbb{R}^{2nm}$ the equations (8) are m equations on the real algebraic set $\mathbb{C}^{nm} \times \mathcal{D}$ and next we prove that imposing these equations decreases the dimension of $\mathbb{C}^{nm} \times \mathcal{D}$ by at least m: Note that it suffices to prove that imposing the equation (8) on $\mathbb{C}^{nm}$, for fixed $X \in \mathcal{D}$, decreases the dimension by at least m. But for

[5] π_1 maps semi-algebraic sets to semi-algebraic sets and does not increase the dimension. See Theorem 2.2.1 and Proposition 2.8.6 of [25].

[6] Here $[x]$:=largest integer i such that $i \leq x$.

fixed $X \in \mathcal{D}$, the i-th equation of (8) just involves the variables of the i-th factor in $(\mathbb{C}^n)^m$. Thus it suffices to prove that for given $X \in \mathcal{D}$ imposing the equation

$$p(v) := v^\dagger X v = 0,\ v \in \mathbb{C}^n, \tag{9}$$

on $\mathbb{C}^n \simeq \mathbb{R}^{2n}$ decreases the dimension by at least one. But for given $X \in \mathcal{D}$ there is $v \in \mathbb{C}^n$ such that $p(v) = v^\dagger X v = \mathrm{tr}(X v v^\dagger) \neq 0$ because $H(\mathbb{C}^n)$ has a basis of rank one operators and $X \neq 0$. Thus, (9) is a non-trivial algebraic equation on the irreducible algebraic set $\mathbb{C}^n \simeq \mathbb{R}^{2n}$. But this immediately implies that (9) does decrease the dimension [7].

Let $\mathcal{M}$ be the algebraic subset of $\mathbb{C}^{nm} \times \mathcal{D}$ obtained by imposing the equations (8) and denote by $\pi_1 : \mathbb{C}^{nm} \times \mathcal{D} \to \mathbb{C}^{nm}$ the canonical projection on the first factor. For $m > \dim \mathcal{D} = 4r(n-r) - 1$, we find $\dim \pi_1(\mathcal{M}) < \dim \mathbb{C}^{nm} = 2nm$ since imposing the equations (8) on $\mathbb{C}^{nm}$ decreases the dimension by at least m. Thus, we conclude that $\pi_1(\mathcal{M})$ has Lebesgue measure zero [8] in $\mathbb{C}^{nm}$. Hence, the subset of $F \in \mathbb{C}^{nm}$ for which $h_F|_{\mathcal{P}_r^n}$ is injective has full Lebesgue measure. Note, that the subset of frames in $\mathbb{C}^{nm}$ has full Lebesgue measure for $m \geq n$. Choosing the measure on the set of frames to be the restriction of the Lebesgue measure, also the subset of frames for which M_F is injective has full measure. □

For $r = 1$, this is the phase retrieval problem and in this case Theorem IV.1 reproduces the main result of [16].

Corollary IV.2. *Let $m \geq 4n - 4$. For almost all frames $F = \{v_1, .., v_m\}$ the map M_F is injective.*

Proof. Let $F = \{v_1, ..., v_m\},\ v_i \in \mathbb{C}^n$, and consider the equations

$$|\langle v_i, x\rangle|^2 - |\langle v_i, y\rangle|^2 = v_i^\dagger (x x^\dagger - y y^\dagger) v_i = 0,\ i \in \{1, ..., m\},$$

in $x, y, v_i \in \mathbb{C}^n$ where $x x^\dagger - y y^\dagger \neq 0$. These equations determine the subset N of $F \in \mathbb{C}^{nm} \simeq \mathbb{R}^{2nm}$ for which M_F fails to be injective. It is easily seen that the equations

$$v_i^\dagger X v_i = 0,\ i \in \{1, ..., m\}, \tag{10}$$

where $X \in \Delta(\mathcal{P}_1^n) - \{0\}$, determine the same subset N. But the equations (10) are precisely the equations (8) for $r = 1$. Thus, the proof can be concluded by going along the lines of the proof of Theorem IV.1. □

A similar result holds true for tight frames.

Theorem IV.3. *(Low-Rank Matrix Recovery with Tight Frames.) If $k(m-1) \geq 4r(n-r) - 1$, then for almost all collections of tight frames $F_1, \ldots, F_k$, with $|F_i| = m$ for all $i \in \{1, \ldots, k\}$, the mapping $(h_{F_1}, \ldots, h_{F_k})|_{\mathcal{P}_r(\mathbb{C}^n)}$ is injective.*

The proof of this Theorem relies on Lemma VI.1 which is our main technical result. Therefore we relegate its proof to Section VIII.

---

[7] Every proper algebraic subset of the irreducible algebraic set $\mathbb{R}^{2m}$ has dimension less than $2m$.
[8] The Lebesgue measure on $\mathbb{R}^n$ is a rescaling of the n-dimensional Hausdorff-measure.

V. STABILITY

The measurement schemes obtained by the method presented in Section III typically come with a stability property. Let

$$\mathcal{M}(n_1,...,n_k) := \{M := (P^1,...,P^k) : \ P^i \text{ POVM with } \dim P^i = n_i\}.$$

In this section we denote $\mathcal{M}(n_1,...,n_k)$ by $\mathcal{M}$. We equip $\mathcal{M}$ with the topology induced by the metric

$$d(M,M') := \|h_M - h_{M'}\| = \sup_{X\in H(\mathbb{C}^n)} \frac{\|h_M(X) - h_{M'}(X)\|_2}{\|X\|_2}$$

where $M, M' \in \mathcal{M}$.

Definition V.1. *Let $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a subset. An $\mathcal{R}$-complete measurement scheme $M \in \mathcal{M}$ is stably $\mathcal{R}$-complete if there exists a neighbourhood $\mathcal{N}$ of M such that every measurement scheme $M' \in \mathcal{N}$ is $\mathcal{R}$-complete.*

Let $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a subset and let $\mathcal{D} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a semi-algebraic set that represents $\Delta(\mathcal{R}) - \{0\}$. Consider the semi-algebraic map

$$\begin{aligned} \psi : \mathcal{D} &\to H(\mathbb{C}^n) \\ X &\mapsto \frac{X}{\|X\|_2}. \end{aligned} \tag{11}$$

By Proposition 2.2.7 and Theorem 2.8.8 of [25], $\tilde{\mathcal{D}} := \psi(\mathcal{D})$ is semi-algebraic with $\dim \tilde{\mathcal{D}} \leq \dim \mathcal{D}$. Furthermore $\tilde{\mathcal{D}}$ clearly represents $\Delta(\mathcal{R}) - \{0\}$.

Lemma V.1. *If $\tilde{\mathcal{D}}$ is closed, every $\mathcal{R}$-complete measurement scheme $M \in \mathcal{M}$ is stably $\mathcal{R}$-complete.*

Proof. Note that $\tilde{\mathcal{D}} \subseteq SH(\mathbb{C}^n)$. $SH(\mathbb{C}^n)$ is compact and thus $\tilde{\mathcal{D}}$ is compact being a closed subset of a compact set. By the continuity of the induced map h_M and compactness of $\tilde{\mathcal{D}}$, $\kappa := \min_{X\in\tilde{\mathcal{D}}} \|h_M(X)\|_2$ exists and $\kappa > 0$ since M is $\mathcal{R}$-complete. Now let $B(M,\kappa/2) := \{M' \in \mathcal{M} : \sup_{X\in SH(\mathbb{C}^n)} \|h_M(X) - h'_M(X)\|_2 < \kappa/2\}$ and note that $B(M,\kappa/2)$ is open. But then

$$\begin{aligned} \min_{X\in\tilde{\mathcal{D}}} \|h_{M'}(X)\| &\geq \min_{X\in\tilde{\mathcal{D}}} \|h_M(X)\|| - \min_{X\in\tilde{\mathcal{D}}} \|h_{M'}(X) - h_M(X)\| \\ &\geq \min_{X\in\tilde{\mathcal{D}}} \|h_M(X)\|| - \max_{X\in\tilde{\mathcal{D}}} \|h_{M'}(X) - h_M(X)\| \\ &\geq \kappa - \max_{X\in SH(\mathbb{C}^n)} \|h_{M'}(X) - h_M(X)\| \\ &\geq \kappa - \kappa/2 = \kappa/2. \end{aligned}$$

Thus all measurement schemes $M' \in B(M,\kappa/2)$ are $\mathcal{R}$-complete. □

Remark Note that $\tilde{\mathcal{D}}$ need not be closed for this lemma to apply: In the situations presented in the following the conclusions solely depend on the dimension of $\tilde{\mathcal{D}}$. By Proposition 2.8.2 of [25] the dimension of $\tilde{\mathcal{D}}$ coincides with the dimension of its closure $\overline{\tilde{\mathcal{D}}}$ in the norm topology on $H(\mathbb{C}^n)$. Furthermore, by Proposition 2.2.2 of [25], the closure of a semi-algebraic set is semi-algebraic. Thus $\overline{\tilde{\mathcal{D}}}$ represents $\Delta(\mathcal{R}) - \{0\}$ and $\dim \overline{\tilde{\mathcal{D}}} \leq \dim \mathcal{D}$.

VI. QUANTUM TOMOGRAPHY WITH VON NEUMANN MEASUREMENTS

Universality of Rank One POVMs

The following lemma is the main technical result of this paper. It asserts that the equations (7) are independent when restricting to rank one POVMs. More precisely let $\mathcal{H} = \mathbb{C}^n$ and denote by $\{e_i\}_{i\in\{1,\dots,n\}}$ the standard basis of $\mathbb{C}^n$.

For a fixed non-zero $X \in H(\mathbb{C}^n)$, consider the equations

$$\begin{aligned} p_i^j(M_1,\dots,M_k) &:= \operatorname{tr}(M_i^\dagger e_j e_j^\dagger M_i X) = e_j^\dagger M_i X M_i^\dagger e_j = 0, \\ &\qquad i \in \{1,...,k\},\ j \in \{1,...,m\}, \\ q_i^{jl}(M_1,\dots,M_k) &:= e_j^\dagger M_i^\dagger M_i e_l - \delta_{jl} = 0, \\ &\qquad i \in \{1,...,k\},\ j,l \in \{1,...,n\}, \end{aligned} \tag{12}$$

in $(M_1,\dots,M_k) \in \Pi_{i=1}^k M(m,n,\mathbb{C})$. Under the canonical identification $M(m,n,\mathbb{C}) \simeq \mathbb{R}^{2nm}$, these can be considered as real algebraic equations in the $2knm$ variables $(M_1,...,M_k)$.

Lemma VI.1. *Let $X \in H(\mathbb{C}^n)$ with $X \neq 0$. Imposing the equations (12) on $\Pi_{i=1}^k M(m,n,\mathbb{C})$ decreases the dimension by at least $kn^2 + k(m-1)$.*

Remark Regarding $X \in \mathcal{D} \subseteq H(\mathbb{C}^n)$ as an variable, the equations (12) can be considered as equations on $\prod_{i=1}^k M(m,n,\mathbb{C}) \times \mathcal{D}$. Then, Lemma VI.1 implies that imposing the equations (12) on $\prod_{i=1}^k M(m,n,\mathbb{C}) \times \mathcal{D}$ decreases the dimension by at least $n^2 + k(m-1)$ for every semi-algebraic set $\mathcal{D} \subseteq H(\mathbb{C}^n)$ with $0 \notin \mathcal{D}$.

Since the proof of this result is rather technical we relegate it to Section VIII. Lemma VI.1 allows us to prove the main theorem of this section.

Theorem VI.2. *(Universality) For $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ a subset, let $\mathcal{D}$ be a semi-algebraic set that represents $\Delta(R) - \{0\}$. If $k(m-1) > \dim \mathcal{D}$, almost all measurement schemes $M \in \mathcal{M}_{1,k}^m(\mathbb{C}^n)$ are stably $\mathcal{R}$-complete.*

Remark Note that Theorem VI.2 reduces the problem of finding an $\mathcal{R}$-complete rank one POVM for some subset $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ to finding a semi-algebraic subset $\mathcal{D} \subseteq H(\mathcal{H})$ which represents $\Delta(\mathcal{R}) - \{0\}$ and in this sense Theorem VI.2 guarantees the universality of rank one POVMs. Furthermore the quality of the result solely depends on the algebraic dimension of $\mathcal{D}$.

The proof of this result can be found in Section VIII.

From this Theorem we directly obtain a Whitney type embedding result for rank one POVMs. Essentially, it is a direct consequence of the following lemma.

Lemma VI.3. *Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a semi-algebraic subset. Then* $\dim(\Delta(\mathcal{R}) - \{0\}) \leq 2 \dim \mathcal{R}$.

Proof. We can assume w.l.o.g that $\mathcal{R}$ is algebraic, because if not we can take its Zariski closure [9]. Let $\mathrm{Diag}(\mathcal{R}\times\mathcal{R}) := \{(X,Y)\in\mathcal{R}\times\mathcal{R} : X = Y\}$. Noting that $\mathrm{Diag}(\mathcal{R}\times\mathcal{R})$ is an algebraic set, $\mathcal{D} := (\mathcal{R}\times\mathcal{R}) - \mathrm{Diag}(\mathcal{R}\times\mathcal{R})$ is quasi-algebraic. But the semi-algebraic map

$$\begin{aligned}\phi : \mathcal{D} &\to \Delta(\mathcal{R}) - \{0\}\\ (X_1, X_2) &\mapsto X_1 - X_2\end{aligned}$$

is surjective, and thus $\dim(\Delta(\mathcal{R}) - \{0\}) \leq \mathcal{D} = 2\dim\mathcal{R}$ by Theorem 2.8.8 of [25]. □

Corollary VI.4. *Let $\mathcal{R}\subseteq\mathcal{S}(\mathbb{C}^n)$ be a subset. If $k(m-1) > 2\dim\mathcal{R}$, almost all measurement schemes $M\in\mathcal{M}^m_{1,k}(\mathbb{C}^n)$ are stably $\mathcal{R}$-complete.*

Proof. We can assume w.l.o.g. that $\mathcal{R}$ is algebraic because if not we can consider its Zariski closure. By the proof of Lemma VI.3, $\Delta(\mathcal{R})-\{0\}$ is semi-algebraic and furthermore $\dim(\Delta(\mathcal{R}) - \{0\}) \leq 2\dim\mathcal{R}$. Finally, Theorem VI.2 with $\mathcal{D} = \Delta(\mathcal{R}) - \{0\}$ concludes the proof. □

Two special cases of this Theorem may be of particular interest.

Corollary VI.5. *Let $\mathcal{R}\subseteq\mathcal{S}(\mathbb{C}^n)$ be a subset. If $k(n-1) > 2\dim\mathcal{R}$, almost all tuples of k von Neumann measurement $M\in\mathcal{M}^k_{vN}(\mathbb{C}^n)$ are $\mathcal{R}$-complete.*

Proof. This immediately follows from Corollary VI.4 for $m = n$. □

Corollary VI.6. *Let $\mathcal{R}\subseteq\mathcal{S}(\mathbb{C}^n)$ be a subset. If $m - 1 > 2\dim\mathcal{R}$, almost all rank one POVMs $M\in\mathcal{M}^m_1(\mathbb{C}^n)$ are stably $\mathcal{R}$-complete.*

Proof. This immediately follows from Corollary VI.4 for $k = 1$. □

Remark Effectively we have the bound $m - 1 > \max\{2\dim\mathcal{R}, n-2\}$ which is due to the fact that a rank one POVM on $\mathbb{C}^n$ has to be at least n-dimensional. If we relax this to merely requiring the POVM to be projective this shortcoming can be avoided, i.e. for projective POVMs $m - 1 = 2\dim\mathcal{R} + 1$ can be attained. This can be seen by modifying the proof of Lemma VI.1.

Rank One POVMs for States of Bounded Rank and States of Fixed Spectrum

In this section we improve the Whitney type bounds of Corollary VI.4 for the cases in which the subset $\mathcal{R}\subseteq\mathcal{S}(\mathcal{H})$ is given by the states of bounded rank or the states of fixed spectrum. The results we obtain in this section easily follow from theorem VI.2. Let us note that all results of this section can be immediately transferred to measurement schemes which fulfil a universality property analogous to theorem VI.2.

In the following, $r\in\{1,...,[n/2]\}$. Denote by $S_r(\mathcal{H})$ the states with rank at most r, i.e. $S_r(\mathcal{H}) := \{\varrho\in\mathcal{S}(\mathcal{H}) : \mathrm{rank}(\varrho)\leq r\}$. We write S^n_r as shorthand for $S_r(\mathbb{C}^n)$.

In analogy to the proof of Theorem IV.1, we first construct the set we use to represent $\Delta(S_r(\mathcal{H})) - \{0\}$ and determine its dimension.

[9] The algebraic dimension is invariant under taking the Zariski closure, see Proposition 2.8.2 of [25]

Lemma VI.7. *The set* $\mathcal{D} := \{X \in \mathcal{P}_{2r}(\mathcal{H}) : \ tr(X) = 0, \ tr(X^2) = 2\}$ *is an algebraic set that represents* $\Delta(S_r(\mathcal{H})) - \{0\}$ *and* $\dim \mathcal{D} = 4r(\dim \mathcal{H} - r) - 2$.

Proof. Note that $\mathcal{S}_r(\mathcal{H}) \subseteq \mathcal{P}_r(\mathcal{H})$ and thus $\Delta(\mathcal{S}_r(\mathcal{H})) \subseteq \Delta(\mathcal{P}_r(\mathcal{H})) = \mathcal{P}_{2r}(\mathcal{H})$. $\mathcal{P}_{2r}(\mathcal{H})$ is algebraic by Lemma II.1 and hence $\mathcal{P}_{2r}(\mathcal{H}) - \{0\}$ represents $\Delta(\mathcal{S}_r(\mathcal{H})) - \{0\}$. In fact $\Delta(\mathcal{S}_r(\mathcal{H})) - \{0\}$ can be represented by a smaller set. Namely one can consider set $\mathcal{D} := \{X \in \mathcal{P}_{2r}(\mathcal{H}) : \ \|X\|_2^2 = tr(X^2) = 1, \ tr(X) = 0\}$. Note that $\mathcal{D}$ is algebraic by Corollary II.2 and that $0 \notin \mathcal{D}$. The equation $tr(X) = 0$ just considers the fact that states have unit trace. Next consider a measurement scheme M and $X \in \Delta(\mathcal{S}_r(\mathcal{H})) - \{0\}$ such that $h_M(X) = 0$. Then, there is $X' := \frac{X}{\|X\|_2} \in \mathcal{D}$ such that $h_M(X') = 0$. Hence $\mathcal{D}$ indeed represents $\Delta(\mathcal{S}_r(\mathcal{H}))-\{0\}$. Finally, by Corollary II.2, we have $\dim(\mathcal{D}) = \dim(\mathcal{P}_{2r}(\mathcal{H}))-2 = 4r(n-r)-2$. □

Theorem VI.8. *If* $k(m-1) \geq 4r(n-r)-1$, *almost all measurement schemes* $M \in M_{1,k}^m(\mathbb{C}^n)$ *are stably* $\mathcal{S}_r^n$*-complete.*

Proof. Using the set of Lemma VI.7 to represent $\Delta(\mathcal{R}) - \{0\}$, the result follows directly form Theorem VI.2. □

As explained in Section IV.A of [2], the lower bounds on the immersion dimension of complex flag manifolds of [26] transfer to lower bounds on the dimension of $\mathcal{S}_r(\mathcal{H})$-complete POVMs. In addition, the discussion following this explanation suggests that the upper bound on m we obtain here is close to optimal.

Next, let us state some corollaries of this theorem.

Corollary VI.9. *If* $m(n-1) \geq 4r(n-r)-1$, *almost all tuples of* k *von Neumann measurements* $M \in \mathcal{M}_{vN}^m(\mathbb{C}^n)$ *are stably* $\mathcal{S}_r^n$*-complete.*

Proof. This follows from Theorem VI.8 for $m = n$. □

For $r = 1$ this reproduces the main result of [11]. In Table I you can see how this result compares to the lower bounds of [26] for some explicit scenarios.

Corollary VI.10. *If* $m - 1 \geq 4r(n-r)-1$, *almost all rank one POVM* $P \in \mathcal{M}_1^m(\mathbb{C}^n)$ *are stably* $\mathcal{S}_r^n$*-complete.*

Proof. This follows from VI.8 for $k = 1$. □

Finally we consider states of fixed spectrum. Let s [10] be a spectrum on $\mathbb{C}^n$ and denote by $\mathcal{S}_s^n \subseteq \mathcal{S}(\mathbb{C}^n)$ the states with spectrum s.

Corollary VI.11. *Let* s *be a spectrum on* $\mathbb{C}^n$ *such that the highest multiplicity of an eigenvalue in* s *is* $n - r$. *Then, if* $k(n-1) \geq 4r(n-r)-1$, *almost all tuples of* k *von Neumann measurements* $M \in \mathcal{M}_{vN}^k(\mathbb{C}^n)$ *are stably* $\mathcal{S}_s^n$*-complete.*

[10] A spectrum on $\mathbb{C}^n$ is a multiset of n increasingly ordered positive real numbers that sum up to one. We call the elements of s eigenvalues.

l\k	2	3	4
5	6/7		
6	6/7		
7	7/7	9/10	
8	7/7	9/10	
9	7/8	9/10	12/12
10	7/8	10/10	12/13

TABLE I: Lower bounds on the minimal number of von Neumann measurements necessary to discriminate any two quantum states of rank at most k from [26] for $\mathcal{S}_k^{k+l}$./ Upper bounds on the minimal number of von Neumann measurements necessary to discriminate any two quantum states of rank at most k from Corollary VI.9 for $\mathcal{S}_k^{k+l}$.

Proof. This follows directly from Theorem VI.8 for $m = n$ noting that $\Delta(\mathcal{S}_s^n) - \{0\}$ can be represented by the set of Lemma VI.7 [11]. □

Corollary VI.12. *Let s be a spectrum on $\mathbb{C}^n$ such that the highest multiplicity of an eigenvalue in s is $n-r$. Then, if $m - 1 \geq 4r(n-r) - 1$, almost all POVMs $P \in M_1^m(\mathbb{C}^n)$ are stably $\mathcal{S}_s^n$-complete.*

Proof. This follows directly from Theorem VI.8 for $k = 1$ noting that $\Delta(\mathcal{S}_s^n) - \{0\}$ can be represented by the set of Lemma VI.7. □

VII. QUANTUM TOMOGRAPHY WITH LOCAL OBSERVABLES

In this section we address the problem of reconstructing states of multipartite systems from the expectation values of local observables.

Let $\mathcal{H} = \bigotimes_{i=1}^k \mathbb{C}^{n_i}$ and let $n := \prod_{i=1}^k n_i$. We define the set $H_{loc}(\mathcal{H})$ of local observables on $\mathcal{H}$ by

$$H_{loc}(\mathcal{H}) := \{O_1 \otimes ... \otimes O_k : O_i \in SH(\mathbb{C}^{n_i})\} \subseteq H(\mathcal{H}).$$

Just like a POVM, a tuple of observables $O := (O_1, ..., O_m) \in H(\mathcal{H})^m$, induces a linear map $h_O : H(\mathcal{H}) \to \mathbb{R}^m,\ X \mapsto (\mathrm{tr}(O_1 X), ..., \mathrm{tr}(O_m X))$ and hence Definition II.3 and Definition V.1 naturally generalize to finite tuples of observables.

The following theorem is the analogue of Theorem VI.2 and it is the main result of this section.

[11] For more details see Lemma IV.3 of [2].

Theorem VII.1. *(Universality) For $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ let $\mathcal{D} \subseteq H(\mathcal{H})$ be a semi-algebraic set that represents $\Delta(\mathcal{R}) - \{0\}$. If $m > \dim \mathcal{D}$, almost all $O \in H_{loc}(\mathcal{H})^m$ are stably $\mathcal{R}$-complete.*

The proof of this Theorem is given in Section VIII.

Again, we directly obtain a Whitney type embedding result for subsets $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ if the measurement consists of determining expectation values of local observables.

Corollary VII.2. *Let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a subset. If $m > 2 \dim \mathcal{R}$, almost all $O \in H_{loc}(\mathcal{H})^m$ are stably $\mathcal{R}$-complete.*

Proof. We can assume w.l.o.g. that $\mathcal{R}$ is algebraic because if not we can consider its Zariski closure. By the proof of Lemma VI.3, $\Delta(\mathcal{R}) - \{0\}$ is semi-algebraic and $\dim(\Delta(\mathcal{R}) - \{0\}) \leq 2 \dim \mathcal{R}$. Finally, Theorem VII.1 concludes the proof. □

Just like in the case of rank one POVMs also this measurement scheme applies to the problem of discriminating states of bounded rank or states of fixed spectrum.

Corollary VII.3. *If $m \geq 4r(n-r) - 1$, almost all $O \in H_{loc}(\mathcal{H})^m$ are stably $\mathcal{S}_r(\mathcal{H})$-complete.*

Proof. Let $\mathcal{D}$ be the quasi-algebraic set of Lemma VI.7. Then the result follows directly from Theorem VII.1. □

Corollary VII.4. *Let s be a spectrum on $\mathcal{H}$ such that the highest multiplicity of an eigenvalue in s is $n-r$. If $m \geq 4r(n-r) - 1$, almost all $O \in H_{loc}(\mathcal{H})^m$ are stably $\mathcal{S}_s^n$-complete.*

Proof. This follows directly from Corollary VII.3 noting that the set of Lemma VI.7 represents $\Delta(\mathcal{S}_s^n) - \{0\}$. □

Finally, let us apply Theorem VII.1 to local Pauli observables on qubit systems. Let $\mathcal{H} = \bigotimes_{i=1}^d \mathbb{C}^2$. The set of local Pauli observables $H_\sigma(\mathcal{H})$ on $\mathcal{H}$ is given by

$$H_\sigma(\mathcal{H}) := \{\sigma_1 \otimes ... \otimes \sigma_d : \sigma_i \in SH(\mathbb{C}^{n_i})_0\}$$

where $H(\mathbb{C}^{n_i})_0 := \{X \in H(\mathbb{C}^{n_i})_0 : \mathrm{tr}(X) = 0\}$ is the real vector space of traceless hermitian $n_i \times n_i$ matrices and $SH(\mathbb{C}^{n_i})_0 := \{X \in H(\mathbb{C}^{n_i})_0 : \|X\|_2 = 1\}$ is the unit sphere in $H(\mathbb{C}^{n_i})_0$.

Corollary VII.5. *If $m \geq 4r(2^d - r) - 1$, almost all $O \in H_\sigma(\mathcal{H})^m$ are stably $\mathcal{S}_r(\mathcal{H})$-complete.*

Proof. Theorem VII.1 also holds for $H_\sigma(\mathcal{H})$ [12]. The remainder of the proof is then along the lines of the proof of Corollary VII.3. □

[12] See the remark after proof of Lemma VIII.3.

VIII. TECHNICAL RESULTS

Proof of Lemma VI.1

Before giving the proof of Lemma VI.1 let us first explain the methods we use to compute the dimension of the relevant algebraic set.

We take advantage of the fact that the dimension of an algebraic set V is given by the dimension of the tangent space at non-singular points of V(see Definition 3.3.3 of [25]). Let us make this more precise: Let $\mathbb{R}[x_1, ..., x_n]$ be the ring of real polynomials in n variables and denote by dp the differential of a real polynomial $p \in \mathbb{R}[x_1, ..., x_n]$, i.e. $dp(y) = \sum_{i=1}^{n} \frac{\partial p}{\partial x_i}|_y dx_i$. Let V_I be the real common zero locus of a set of real polynomials $I := \{p_1, ..., p_m\} \subseteq \mathbb{R}[x_1, ..., x_n]$. For all $x \in V_I$,

$$\sum_{i=1}^{m} \alpha_i dp_i(x) = 0 \tag{13}$$

gives a system of linear equations in $\alpha_1, ..., \alpha_m \in \mathbb{R}$. In the following we mainly use the following facts:

1. The rank of the system of linear equations (13) at a non-singular point of V_I is given by $n - d$ where d is the dimension of V_I [13].

2. The non-singular points of V_I are an algebraic subset of dimension less than d by Proposition 3.3.14 of [25].

.

By computing these systems of linear equations, we prove that for a given non-zero $X \in H(\mathbb{C}^n)$, imposing the equations (12) on $\Pi_{i=1}^{k} M(m, n, \mathbb{C})$ decreases the dimension by at least $n^2 + k(m-1)$.

First, let us state a lemma which allows us to efficiently compute the systems of linear equations for the equations (12). Let $A \in M(s, m, \mathbb{R})$, $C \in M(m, t, \mathbb{R})$, $B \in H(\mathbb{C}^n)$. Furthermore, identify $M(m, n, \mathbb{C})$ with $\mathbb{R}^{2mn}$ via the canonical map $\iota : M(m, n, \mathbb{C}) \to \mathbb{R}^{2mn}$, $Y \mapsto (\mathrm{Re}(Y), \mathrm{Im}(Y))$. Then the equations

$$p_{lo}^I(Y) := \mathrm{Im}(AYBY^\dagger C)_{lo} = 0, \quad p_{lo}^R(Y) := \mathrm{Re}(AYBY^\dagger C)_{lo} = 0,$$
$$l \in \{0, ..., s\}, o \in \{0, ..., t\},$$

can be considered as real algebraic equations in the variables $y_{jk}^R := (\mathrm{Re}(Y))_{jk}, y_{jk}^I := (\mathrm{Im}(Y))_{jk}$, $j \in \{0, ..., m\}, k \in \{0, ..., n\}$.

Lemma VIII.1. *Let $Y \in M(m, n, \mathbb{C})$ be such that $AYBY^\dagger C = 0$. Then, the system of linear equations*

$$L(Y) := \sum_{l=1}^{s} \sum_{o=1}^{t} \left(\alpha_{lo}^R dp_{lo}^R(Y) + \alpha_{lo}^I dp_{lo}^I(Y) \right) = 0$$

[13] See Definition 3.3.4 and Proposition 3.3.10 of [25].

in $\alpha^R_{lo} \in \mathbb{R},\ \alpha^I_{lo} \in \mathbb{R}$ *is equivalent to* $A^T M_\alpha C^T Y B + C M^\dagger_\alpha A Y B = 0$ *where* $(M_\alpha)_{lo} := \alpha^R_{lo} + i\alpha^I_{lo},\ l \in \{0,...,s\}, o \in \{0,...,t\}$.

Proof. Let

$$L_{jk} = (\partial_{y^R_{jk}} - i\partial_{y^I_{jk}}) \sum_{l=1}^{s}\sum_{o=1}^{t} \left(\alpha^R_{lo}\, p^R_{lo} + \alpha^I_{lo}\, p^I_{lo}\right),\ j \in \{1,...,m\}, k \in \{1,...,n\}.$$

Then the system of linear equations $\{L_{jk}(Y) = 0\}_{j\in\{1,...,m\},k\in\{1,...,n\}}$ is equivalent to $L(Y) = 0$ since

$$\begin{aligned}
L &= \sum_{l=1}^{s}\sum_{o=1}^{t}\left(\alpha^R_{lo}\sum_{j=1}^{m}\sum_{k=1}^{n}\left((\partial_{y^R_{jk}} p^R_{lo})dy^R_{jk} + (\partial_{y^I_{jk}} p^R_{lo})dy^I_{jk}\right) + \alpha^I_{lo}\sum_{j=1}^{m}\sum_{k=1}^{n}\left((\partial_{y^R_{jk}} p^I_{lo})dy^R_{jk} + (\partial_{y^I_{jk}} p^I_{lo})dy^I_{jk}\right)\right)\\
&= \sum_{j=1}^{m}\sum_{k=1}^{n}\left(\left(\partial_{y^R_{jk}}\sum_{l=1}^{s}\sum_{o=1}^{t}\left(\alpha^R_{lo}\, p^R_{lo} + \alpha^I_{lo}\, p^I_{lo}\right)\right)dy^R_{jk} + \left(\partial_{y^I_{jk}}\sum_{l=1}^{s}\sum_{o=1}^{t}\left(\alpha^R_{lo}\, p^R_{lo} + \alpha^I_{lo}\, p^I_{lo}\right)\right)dy^I_{jk}\right)\\
&= \sum_{j=1}^{m}\sum_{k=1}^{n}\left(\mathrm{Re}(L_{jk})dy^R_{jk} - \mathrm{Im}(L_{jk})dy^I_{jk}\right).
\end{aligned}$$

Let $\partial_{y_{jk}} = \partial_{y^R_{jk}} - i\partial_{y^I_{jk}}$ and note that $\partial_{y_{jk}} Y_{lm} = 2\delta_{jl}\delta_{km}$, $\partial_{y_{jk}} Y^*_{lm} = 0$. Then,

$$\begin{aligned}
L_{jk}(Y) &= (\partial_{y^R_{jk}} - i\partial_{y^I_{jk}})\sum_{l=1}^{s}\sum_{o=1}^{t}\left(\alpha^R_{lo}\frac{1}{2}(AYBY^\dagger C + AY^*B^*Y^T C)_{lo} + \alpha^I_{lo}\frac{1}{2i}(AYBY^\dagger C - AY^*B^*Y^T C)_{lo}\right)\\
&= \frac{1}{2}\partial_{y_{jk}}\sum_{l=1}^{s}\sum_{o=1}^{t}\left((M^*_\alpha)_{lo}(AYBY^\dagger C)_{lo} + (M_\alpha)_{lo}(AY^*B^*Y^T C)_{lo}\right)\\
&= \sum_{l=1}^{s}\sum_{o=1}^{t}\sum_{p=1}^{m}\sum_{q=1}^{n}\left((M^*_\alpha)_{lo}A_{lp}\delta_{pj}\delta_{qk}(BY^\dagger C)_{qo} + (M_\alpha)_{lo}(AY^*B^*)_{lq}\delta_{qk}\delta_{pj}C_{po}\right)\\
&= (A^T M^*_\alpha C^T Y^* B^T + C M^T_\alpha A Y^* B^*)_{jk}\\
&= (A^T M_\alpha C^T Y B + C M^\dagger_\alpha A Y B)^*_{jk}.
\end{aligned}$$

Hence $L(Y) = 0$ is equivalent to $A^T M_\alpha C^T Y B + C M^\dagger_\alpha A Y B = 0$. □

Under the identification $M(m,n,\mathbb{C}) \simeq \mathbb{R}^{2mn}$ given by the map ι defined above, also the equations

$$r^R_{lo}(Y) := \mathrm{Re}(Y^\dagger Y)_{lo} - \delta_{lo} = 0,\ r^I_{lo}(Y) := \mathrm{Im}(Y^\dagger Y)_{lo} = 0,\quad l,o \in \{1,...,n\},$$

can be considered as real algebraic equations in the variables $y^R_{jk} := (\mathrm{Re}(Y))_{jk}, y^I_{jk} := (\mathrm{Im}(Y))_{jk},\ j \in \{0,...,m\}, k \in \{0,...,n\}$.

Corollary VIII.2. *Let* $Y \in M(m,n,\mathbb{C})$ *be such that* $Y^\dagger Y - \mathbb{1}_n = 0$. *Then, the system of linear equations*

$$L(Y) := \sum_{l,o=1}^{n}\left(\gamma^R_{lo} dr^R_{lo}(Y) + \gamma^I_{lo} dr^I_{lo}(Y)\right) = 0$$

in $\gamma_{lo}^R \in \mathbb{R},\ \gamma_{lo}^I \in \mathbb{R}$ *is equivalent to* $Y(M_\gamma + M_\gamma^\dagger) = 0$ *where* $(M_\gamma)_{lo} := \gamma_{lo}^R + i\gamma_{lo}^I,\ l, o \in \{1, \cdots, n\}$.

Proof. The proof of this result can be obtained by going along the lines of the proof of Lemma VIII.1, so we just give the calculation that differs: $L(Y) = 0$ is equivalent to $\{L_{jk}(Y) = 0\}_{j\in\{1,\cdots,m\},k\in\{1,\cdots,n\}}$ where

$$\begin{aligned}
L_{jk}(Y) &= (\partial_{y_{jk}^R} - i\partial_{y_{jk}^I}) \sum_{l,o=1}^{n} \left(\gamma_{lo}^R \frac{1}{2}(Y^\dagger Y + Y^T Y^*)_{lo} + \gamma_{lo}^I \frac{1}{2i}(Y^\dagger Y - Y^T Y^*)_{lo} \right) \\
&= \frac{1}{2}\partial_{y_{jk}} \sum_{l,o=1}^{n} \left((M_\gamma^*)_{lo}(Y^\dagger Y)_{lo} + (M_\gamma)_{lo}(Y^T Y^*)_{lo} \right) \\
&= \sum_{l,o=1}^{n} \sum_{p=1}^{m} \left((M_\gamma^*)_{lo}\delta_{ko}\delta_{jp}(Y^\dagger)_{lp} + (M_\gamma)_{lo}(Y^*)_{po}\delta_{lk}\delta_{pj} \right) \\
&= (Y^* M_\gamma^* + Y^* M_\gamma^T)_{jk} \\
&= (Y M_\gamma + Y M_\gamma^\dagger)_{jk}^*.
\end{aligned}$$

Hence $L(Y) = 0$ is equivalent to $Y(M_\gamma + M_\gamma^\dagger) = 0$. □

Remark Note that combining the equations of Lemma VIII.1 and Corollary VIII.2 yields the system of linear equations $Y(M_\gamma + M_\gamma^\dagger) + A^T M_\alpha C^T Y B + C M_\alpha^\dagger A Y B = 0$ (see equations 13).

Let us now give the proof of Lemma VI.1.

Proof. For a given non-zero $X \in H(\mathbb{C}^n)$ and $i \in \{1, ..., k\}$, consider the following equations in $(M_1, \ldots, M_k) \in \prod_{i=1}^k M(m, n, \mathbb{C})$:

$$p_i^j(M_1, ..., M_k) := \mathrm{tr}(M_i^\dagger e_j e_j^\dagger M_i X) = e_j^\dagger M_i X M_i^\dagger e_j = 0, \quad j \in \{1, ..., m\},$$

and

$$q_i^{jl}(M_1, ..., M_k) := (M_i^\dagger M_i)_{jl} - \delta_{jl} = 0, \quad j, l \in \{1, ..., n\}.$$

Under the canonical identification $\prod_{i=1}^k M(m, n, \mathbb{C}) \simeq \mathbb{R}^{2knm}$, these equations can be regarded as real algebraic equations in $2knm$ variables. Let $I_i := \{p_i^j\}_{j\in\{1,...,m\}}$ and $J_i := \{q_i^{jl}\}_{j,l\in\{1,...,n\}}$.

We have to show that the dimension of the real common zero locus of the equations $K_k = \bigcup_{i=1}^k I_i \cup J_i$ is at most $2kmn - kn^2 - k(m-1)$. Denote by $\iota_1 : M(m, n, \mathbb{C}) \to \Pi_{i=1}^k M(m, n, \mathbb{C}),\ M \mapsto (M, 0, ...)$ the inclusion in the first factor and let $\pi_i : \Pi_{i=1}^k M(m, n, \mathbb{C}) \to M(m, n, \mathbb{C}),\ (M_1, ..., M_i, ..., M_k) \mapsto M_i$ be the projection on the i-th factor. Then we find $I_i \cup J_i = (J_1 \cup I_1) \circ \iota_1 \circ \pi_i$, where $(J_1 \cup I_1) \circ \iota_1 \circ \pi_i := \{p \circ \iota_1 \circ \pi_i : p \in J_1 \cup I_1\}$. Thus, we conclude that $V_{K_k} \simeq \prod_{i=1}^k V_{K_1}$ and it suffices to reduce to $k = 1$. We stick to the notation introduced in the beginning of this section and denote the algebraic set obtained from $M(m, n, \mathbb{C})$ by imposing the equations $I := I_1$ and $J := J_1$ by $V_{I\cup J}$.

Let us now determine the system of linear equations L associated to $I \cup J$ at $U \in V_{I\cup J}$. The contribution of the j-th equation of I to L is obtained from Lemma VIII.1 by choosing $A = e_j^\dagger$, $B = X$, $C = e_j$, $Y = U$ and thus the contribution of I is given by

$$\sum_{j=1}^{m} \alpha_j^R e_j e_j^\dagger UX,\ \alpha_j^R \in \mathbb{R}.$$

Similarly, by Corollary VIII.2, the contribution of J to L is given by,

$$U(M_\gamma + M_\gamma^\dagger)$$

where $(M_\gamma)_{jk} := \gamma_{jk}^R + i\gamma_{jk}^I, i, j \in \{1, ...n\}, \gamma_{jk}^R, \gamma_{jk}^I \in \mathbb{R}$. Note that this just gives conditions on the hermitian part of M_γ and define $\Gamma \in H(\mathbb{C}^n)$ by $\Gamma := M_\gamma + M_\gamma^\dagger$.

Combining these two parts, the system of linear equations associated to the equations $I \cup J$ at $U \in V_{I\cup J}$ is equivalent to the following system of linear equations in $\alpha_1, ..., \alpha_m \in \mathbb{R}$ and $\gamma_{kj}^R \in \mathbb{R}, \gamma_{kj}^I \in \mathbb{R},\ k, j \in \{1, ..., n\}$,

$$U\Gamma + D_\alpha UX = 0 \tag{14}$$

where $D_\alpha = \sum_{j=1}^m \alpha_j e_j e_j^\dagger$. Observing that Γ is uniquely determined by the equations (14), the rank of (14) is at least n^2 and we can reduce to the anti-hermitian part of (14) to find the remaining $m - 1$ independent equations:

$$0 = U\Gamma U^\dagger + D_\alpha UXU^\dagger - \left(U\Gamma U^\dagger + D_\alpha UXU^\dagger\right)^\dagger = -[UXU^\dagger, D_\alpha]. \tag{15}$$

Next we study the commutator $[UXU^\dagger, D_\alpha]$ in detail. As X is an arbitrary hermitian matrix, we have to carefully consider all possible combinations of eigenspaces, or more precisely eigenspace degeneracies, X could have.

In order to achieve this, let us begin with the following example, which will be the starting point for the decomposition of X: Let M be a subset of $\{1, ..., m\}$ and define the diagonal projection $D_M \in M(m, \mathbb{R})$ by $e_i^\dagger D_M e_j := \delta_{i,j}\delta_{j,M}$, where $\delta_{j,M} = 1$ for $j \in M$ and 0 else. The following observation is the crucial idea for the remainder of the proof: If $[UXU^\dagger, D_M] \neq 0$ for all proper subsets M of $\{1, ..., m\}$ then $m - 1$ of the operators $\{[UXU^\dagger, D_{\{i\}}]\}_{i\in\{1,...,m\}}$ are linearly independent. To show this, assume that there are $a_j \in \mathbb{R},\ j \in \{1, ..., m\}$, with $a_k \neq a_l$ for some k, l such that $\sum_{j=1}^m a_j[UXU^\dagger, D_{\{j\}}] = 0$. Since the commutativity of hermitian matrices is determined solely by their eigenspaces, we deduce $[UXU^\dagger, D_E] = 0$, where $E := \{j \in \{1, ..., m\} : a_j = a_k\}$. But this is a contradiction since E is a proper subset of $\{1, \cdots, m\}$. Hence, the only solution is $a_1 = a_2 = \cdots = a_m$ and this proves the claim. Thus, in this case we conclude that the solution of the system of linear equations (15) is given by $\alpha_1 = ... = \alpha_m$ and hence there are $m - 1$ linearly independent equations.

Next, we decompose $V_{I\cup J}$ into quasi-algebraic subsets for which the argument we just gave can be applied[14]. Let $P[m]$ be the set of partitions of $\{1, ..., m\}$. We say that a subset

[14] By means of this decomposition we can separately consider all possible eigenspace degeneracies of X.

$S \subseteq \{1, ..., m\}$ is subordinate to a partition $P \in P[m]$ if there is $M \in P$ such that S is a proper subset of M. For given $P \in P[m]$, define the quasi-algebraic set W_P to be the set of $U \in V_{I \cup J}$ such that

$$[D_M, UXU^\dagger] = 0, \ \forall M \in P, \tag{16}$$

and

$$[D_N, UXU^\dagger] \neq 0, \ \forall N \subseteq \{1, ..., m\} \text{ subordiante to } P.$$

The set $V_{I \cup J}$ can clearly be decomposed into the sets W_P:

$$V_{I \cup J} = \bigcup_{P \in P[m]} W_P.$$

Having already checked that $2mn - \dim W_P = m - 1 + n^2$ if P is the trivial partition, we conclude the proof by showing that $2mn - \dim W_P \geq m - 1 + n^2$ for all non-trivial $P \in P[m]$ [15]. In order to prove this, we first show that the rank of the system of linear equations associated to W_P is at least $n^2 + m - 1$ for all points in W_P.

Let $P = \{M_1, ..., M_l, M_{l+1}\} \in P[m]$ be an arbitrary non-trivial partition. Choosing $A = D_{M_j}$, $B = X$, $C = \mathrm{id}_m$ and $Y = U$ in Lemma VIII.1 yields

$$D_{M_j} M_{\beta_j} UX + M_{\beta_j}^\dagger D_{M_j} UX,$$

where $M_{\beta_j} \in M(m, \mathbb{C})$ with $(M_{\beta_j})_{lo} := \beta_{j;lo}^R + i\beta_{j;lo}^I, \ l, o \in \{1, ..., m\}, \ \beta_{j;lo}^R, \beta_{j;lo}^I \in \mathbb{R}$ and similarly with the roles of A and C exchanged. Thus, equation (16) for M_j gives the following contribution to the system of linear equations associated to W_P at $U \in W_P$:

$$[D_{M_j}, M_{\beta_j} - M_{\beta_j}^\dagger] UX.$$

Thus, the system of linear equations associated to W_P at $U \in W_P$ is equivalent to the following system of linear equations in $\alpha_1, ..., \alpha_m \in \mathbb{R}$, $\gamma_{kj}^R \in \mathbb{R}, \gamma_{kj}^I \in \mathbb{R}, \ k, j \in \{1, ..., n\}$, and $\beta_{j;lo}^R \in \mathbb{R}, \beta_{j;lo}^I \in \mathbb{R}, \ j \in \{1, ..., l+1\}, l, o \in \{1, ..., m\}$:

$$U\Gamma + D_\alpha UX + \sum_{k=1}^{l+1} [D_{M_k}, M_{\beta_k} - M_{\beta_k}^\dagger] UX = 0.$$

Again, we can eliminate Γ by reducing to the anti-hermitian part to obtain

$$U\Gamma U^\dagger + D_\alpha UXU^\dagger + \sum_{k=1}^{l+1} [D_{M_k}, M_{\beta_k}^H] UXU^\dagger - \left(U\Gamma U^\dagger + D_\alpha UXU^\dagger + \sum_{k=1}^{l+1} [D_{M_k}, M_{\beta_k}^H] UXU^\dagger \right)^\dagger$$

$$\Leftrightarrow [UXU^\dagger, D_\alpha] + \sum_{k=1}^{l+1} [UXU^\dagger, [M_{\beta_k}^H, D_{M_k}]] = 0, \tag{17}$$

[15] Note that, depending on the choice of X, many of the W_P might be empty. If $X = \mathbb{1}_n$, $n = m$ for instance, all W_P would be empty.

where $M^H_{\beta_j}$ is the anti-hermitian $m \times m$ matrix defined by $M^H_{\beta_j} := M_{\beta_j} - M^\dagger_{\beta_j}$.

Conjugating with D_{M_j} yields

$$[UXU^\dagger, D_{M_j} D_\alpha] = 0,$$

where we used $[UXU^\dagger, D_{M_j}] = 0$ together with $D_{M_j}[M^H_{\beta_k}, D_{M_k}]D_{M_j} = D_{M_j} M^H_{\beta_j} D_{M_j} - D_{M_j} M^H_{\beta_j} D_{M_j} = 0$. By construction of W_P, we have $[UXU^\dagger, D_{M_j} D_M] \neq 0$ for all proper subsets $M \subseteq M_j$. Since the commutativity of hermitian matrices is solely determined by their eigenspaces we conclude just like in the case of the trivial partition that $D_{M_j} D_\alpha \propto D_{M_j}$ for all $j \in \{1, ..., l+1\}$ [16]. Thus, if there is $U \in W_P$, the rank of (17) at U is at least $n^2 + m - l - 1$.

To find the remaining l independent equations consider the remaining equations

$$\sum_{j=1}^{l+1} [UXU^\dagger, [M^H_{\beta_j}, D_{M_j}]] = 0.$$

There is $i \in \{1, ..., l+1\}$ with $D_{M_i} UXU^\dagger \neq 0$ because otherwise we would conclude that $UXU^\dagger = 0$ which is a contradiction since $U \in U(m, n)$ and $X \neq 0$ by assumption. Multiplying by D_{M_k} from the left and D_{M_i} from the right yields

$$\begin{aligned}
&\sum_{j=1}^{l} D_{M_k} [UXU^\dagger, [M^H_{\beta_j}, D_{M_j}]] D_{M_i} = 0 \\
\Leftrightarrow &\sum_{j=1}^{l} [UXU^\dagger, D_{M_k} [M^H_{\beta_j}, D_{M_j}]] D_{M_i} = 0 \\
\Leftrightarrow &[UXU^\dagger, D_{M_k} (M^H_{\beta_i} - M^H_{\beta_k}) D_{M_i}] = 0.
\end{aligned}$$

For each $k \in \{1, ..., l+1\} - \{i\}$ this gives at least one equation on $M^H_{\beta_k}$: First, assume $|M_i| = 1$. Then there is $q \in \{1, \ldots, m\}$ such that $M_i = \{q\}$. Furthermore, since

$$0 \neq D_{M_i} UXU^\dagger = D_{M_i} UXU^\dagger D_{M_i} = (e^d_q agger UXU^\dagger q) q q^\dagger,$$

we conclude that $e^\dagger_q UXU^\dagger q \neq 0$. But this is a contradiction to the q-th equation of I.

Hence we can assume $|M_i| \geq 2$. By construction of W_P there is an eigenvector $v_k \neq 0$ of $UXU^\dagger$ in the range of D_{M_k} with eigenvalue λ_k and a eigenvector $v_i \neq 0$ of $UXU^\dagger$ in the range of D_{M_i} with eigenvalue λ_i. Since we assumed $|M_i| \geq 2$, by construction of W_P, $UXU^\dagger$ has at least two eigenvectors in the range of D_{M_i} with different eigenvalues because otherwise there would be a proper subset of $N \subseteq M_i$ such that $[UXU^\dagger, D_N] = 0$. Thus, we can choose λ_i such that $\lambda_i \neq \lambda_k$. We then find

$$\begin{aligned}
&v^\dagger_k [UXU^\dagger, D_{M_k} (M^H_{\beta_i} - M^H_{\beta_k}) D_{M_i}] v_i = 0 \\
\Leftrightarrow &v^\dagger_k (M^H_{\beta_i} - M^H_{\beta_k}) v_i (\lambda_k - \lambda_i) = 0 \\
\Leftrightarrow &v^\dagger_k M^H_{\beta_i} v_i - v^\dagger_k M^H_{\beta_k} v_i = 0.
\end{aligned}$$

[16] In particular, note that if D_α solves the system of linear equations (17) we have $[UXU^\dagger, D_\alpha] = 0$.

But this clearly gives a non-trivial condition on $M^H_{\beta_k}$ since $M^H_{\beta_k} = M_{\beta_j} - M^\dagger_{\beta_j}$. Thus we conclude that, if there is $U \in W_P$, the rank of (17) at U is at least $m-l-1+l = m-1$ and hence the rank of the system of linear equations associated to W_P at U is at least n^2+m-1. But if W_P is non-empty, it does contain a non singular-point by Proposition 3.3.14 of [25]. And thus the rank of the system of linear equations associated to W_P at this non-singular point is at least n^2+m-1. Hence $2kmn - \dim W_P \geq n^2+m-1$ by Proposition 3.3.10 of [25].

□

Proof of Theorem VI.2

Proof. Let ψ be the map defined in (11). We can assume that $\mathcal{D}$ is a closed subset of $SH(\mathbb{C}^n)$ because if not we can replace it by the closure of $\psi(\mathcal{D})$ without increasing its dimension [17]. Let $\tilde{\mathcal{M}} := \{(U_1,...,U_k,X) \in \prod_{i=1}^k U(m,n) \times \mathcal{D} : e_j^\dagger U_i X U_i^\dagger e_j = 0,\ j \in \{1,\dots,m\}, i \in \{1,\dots,k\}\}$.

First, we fix the measure on $\mathcal{M}^m_{1,k}(\mathbb{C}^n)$: Let ϕ be the map defined in equation (1). We define the measure μ on $\mathcal{M}^m_{1,k}(\mathbb{C}^n)$ to be the pushforward measure of the $2knm$-dimensional Hausdroff measure μ_H on $\prod_{i=1}^k U(m,n) \subseteq \mathbb{R}^{2nmk}$, i.e. $\mu(A) := \phi_*(\mu_H)(A) = \mu_H(\phi^{-1}(A))$ for $A \subseteq \mathcal{M}^m_{\text{vN}}(\mathbb{C}^n)$ a measurable set.

Note that ϕ is the quotient projection with respect to the left action of the toral goup $T := \prod_{i=1}^k T(m)$, $T(m) := \{\text{diag}(\lambda_1,...,\lambda_m) : \lambda_i \in U(1)\}$ on $\prod_{i=1}^k U(m,n)$ given by $((U_1,...,U_k),(T_1,...,T_k)) \mapsto ((U_1,...,U_k),(T_1U_1,...,T_kU_k))$. Also note that the equations (12) are invariant under the action of T and hence $T\pi_1(\tilde{\mathcal{M}}) = \pi_1(\tilde{\mathcal{M}})$ where $\pi_1 : \prod_{i=1}^k U(m,n) \times \mathcal{D} \to \prod_{i=1}^k U(m,n)$ is the projection on the first factor. Thus, for $\mu_H(\pi_1(\tilde{\mathcal{M}})) = 0$, we find

$$\begin{aligned}\mu\left(\phi \circ \pi_1(\tilde{\mathcal{M}})\right) &= \mu_H\left(\phi^{-1}\left(\phi \circ \pi_1(\tilde{\mathcal{M}})\right)\right) \\ &= \mu_H\left(T\pi_1(\tilde{\mathcal{M}})\right) \\ &= \mu_H\left(\pi_1(\tilde{\mathcal{M}})\right) = 0.\end{aligned}$$

Hence, it suffices to prove that $\mu_H(\pi_1(\tilde{\mathcal{M}})) = 0$.

Finally, for $k(m-1) > \dim \mathcal{D}$ we find $\dim \pi_1(\tilde{\mathcal{M}}) \leq \dim \prod_{i=1}^k U(m,n) + \dim \mathcal{D} - m(k-1) < \dim \prod_{i=1}^k U(m,n)$ by Lemma VI.1. So $\pi_1(\tilde{\mathcal{M}})$ has μ_H-measure zero in $\prod_{i=1}^k U(m,n)$. The stability follows directly from Lemma V.1. □

Remark Note that by the remark after Lemma VI.1, this proof just depends on $\mathcal{D} \subseteq H(\mathbb{C}^n)$ and hence naturally extends to semi-algebraic subsets $\mathcal{R} \subseteq H(\mathbb{C}^n)$. Furthermore, this proof shows that indeed $\pi_1(\tilde{\mathcal{M}})$ has μ_H-measure zero in $\prod_{i=1}^k U(m,n)$. Thus the statement of Theorem VI.2 naturally also holds for tight frames $U \in U(n,m)$.

[17] See remark after Lemma V.1 for more details.

Proof of Theorem VII.1

For a given non-zero $X \in H(\mathcal{H})$, consider the equations

$$p^i((O_1^1,\dots,O_k^1),\dots,(O_1^m,\dots,O_k^m)) := \mathrm{tr}((O_1^i\otimes\cdots\otimes O_k^i)X) = 0,\ i\in\{1,...,m\}, \quad (18)$$

in $((O_1^1,\dots,O_k^1),\dots,(O_1^m,\dots,O_k^m)) \in (\Pi_{i=1}^k H(\mathbb{C}^{n_i}))^m$. Under the identification $H(\mathbb{C}^{n_i}) \simeq \mathbb{R}^{n_i^2}$, these equations can be considered as real algebraic equations in the variables $((O_1^1,\dots,O_k^1),\dots,(O_1^m,\dots,O_k^m))$. The following Lemma is the analogue of Lemma VI.1.

Lemma VIII.3. *Let $X \in H(\mathcal{H})$ be non-zero. Imposing the equations* (18) *on $(\Pi_{i=1}^k SH(\mathbb{C}^{n_i}))^m$ decreases the dimension by at least m.*

Proof. The equation p_i just involves the variables $(O_1^i,\dots,O_k^i)$ of the i-th factor of $(\Pi_{i=1}^k H(\mathbb{C}^{n_i}))^m$. Thus, it suffices to prove that, for given non-zero $X \in H(\mathcal{H})$, imposing the equation

$$p((O_1,\dots,O_k)) := \mathrm{tr}((O_1\otimes\cdots\otimes O_k)X) = 0 \quad (19)$$

on $\Pi_{i=1}^k SH(\mathbb{C}^{n_i})$ decreases the dimension by at least one.

In order to see that this is true, note that there are $(O_1,\dots,O_k) \in \Pi_{i=1}^k SH(\mathbb{C}^{n_i})$ such that $\mathrm{tr}((O_1\otimes\cdots\otimes O_k)X) \neq 0$ because $\bigotimes_{i=1}^k H(\mathbb{C}^{n_i})$ has a basis of normalized local operators and $X \neq 0$. But then, the equation (19) is a non-trivial algebraic equation on the irreducible algebraic set $\Pi_{i=1}^k SH(\mathbb{C}^{n_i})$ and thus the dimension has to decrease since for a proper algebraic subset V of an irreducible algebraic set W we have $\dim V < \dim W$. □

Remark By going along the lines of the this proof, it is easily seen that Lemma VIII.3 also holds when going from hermitian matrices to traceless hermitian matrices, i.e. if we replace $(\Pi_{i=1}^k SH(\mathbb{C}^{n_i}))^m$ by $(\Pi_{i=1}^k SH(\mathbb{C}^{n_i})_0)^m$. Furthermore, the proof of Theorem VII.1 also holds when going from $(\Pi_{i=1}^k SH(\mathbb{C}^{n_i}))^m$ to $(\Pi_{i=1}^k SH(\mathbb{C}^{n_i})_0)^m$ and considering $H_{loc,0}(\mathcal{H}) := \{O_1\otimes ...\otimes O_k : O_i \in SH(\mathbb{C}^{n_i})_0\}$ instead of $H_{loc}(\mathcal{H})$.

Now we can give the proof of Theorem VII.1.

Proof. Let ψ be the map defined in (11). We can assume that $\mathcal{D}$ is a closed subset of $SH(\mathcal{H})$ because if not we can replace it by the closure of $\psi(\mathcal{D})$ without increasing its dimension [18]. Let $\mathcal{M}$ be the semi-algebraic set obtained from $(\Pi_{i=1}^k H(\mathbb{C}^{n_i}))^m \times \mathcal{D}$ by imposing the equations (18).

For $m > \dim\mathcal{D}$ we get $\dim\pi_1(\mathcal{M}) < \dim(\Pi_{i=1}^k SH(\mathbb{C}^{n_i}))^m$ by Lemma VIII.3.

Now consider $\theta(\pi_1(\mathcal{M}))$ where

$$\theta : (\Pi_{i=1}^k SH(\mathbb{C}^{n_i}))^m \to (H_{loc}(\mathcal{H}))^m,$$
$$(O_1^1,\dots,O_k^1),\dots,(O_1^m,\dots,O_k^m) \mapsto (O_1^1\otimes\cdots\otimes O_k^1),\dots,(O_1^m\otimes\cdots\otimes O_k^m).$$

[18] See remark after Lemma V.1 for more details.

Note that θ is a surjective semi-algebraic map and thus $(H_{loc}(\mathcal{H}))^m$ is semi-algebraic with $\dim((H_{loc}(\mathcal{H}))^m) \leq \dim((\Pi_{i=1}^k SH(\mathbb{C}^{n_i}))^m)$. Furthermore, θ is injective when restricting to positive matrices and hence $d := \dim(H_{loc}(\mathcal{H}))^m = \dim(\Pi_{i=1}^k SH(\mathbb{C}^{n_i}))^m$.

Finally, since $\dim \pi_1(\mathcal{M}) < d$ and θ is semi-algebraic, we have $\dim(\theta(\pi_1(\mathcal{M}))) < d$ and thus $\theta(\pi_1(\mathcal{M}))$ has zero d-dimensional Hausdorff measure. Stability follows directly from Lemma V.1. □

Proof of Theorem IV.3

Proof. By going along the lines of the proof of Lemma VI.7, it is easily seen that $\mathcal{D} := \{X \in \mathcal{P}_{2r}(\mathcal{H}) : \ \mathrm{tr}(X^2) = 2\}$ represents $\Delta(\mathcal{P}_r^n) - \{0\}$ and furthermore we have $\dim \mathcal{D} = 4r(n-r) - 1$ by Corollary II.2 [19]. Applying Theorem VI.2 [20] to the set $\mathcal{D}$ then concludes the proof. □

Appendix A: Hausdorff Measure on Semi-Algebraic Sets

The term "almost" all used in many of the results of this paper refers to the Hausdorff measure on real affine space. In this section we define the Hausdorff measure and we prove the well-known fact that a semi-algebraic set of dimension d has zero $(d+1)$-dimensional Hausdorff measure.

For a non-empty subset $A \subseteq \mathbb{R}^n$ the diameter of S is defined by $\mathrm{diam}(S) := \sup\{\|x - y\|_2 : x, y \in S\}$.

Let $m \in \mathbb{R}$. For an arbitrary subset $S \subseteq \mathbb{R}^n$ the m-dimensional Hausdorff measure $\mu_H^m(S)$ is defined by (see Section 2.3 of [27])

$$\mu_H^m(S) = \lim_{\delta \to 0} \inf\{\sum_{i=1}^{\infty} (\mathrm{diam}(S_i))^m : S \subseteq \cup_{i \in \mathbb{N}}(S_i), \ \mathrm{diam} S_i < \delta\}.$$

Proposition A.1. *Let $m > n$. A semi-algebraic set S of dimension n has zero m-dimensional Hausdorff measure.*

Proof. Every n-dimensional semi-algebraic set S can be expressed as $S = \bigcup_{i=1}^k S_i$ for some $k \in \mathbb{N}$ where the S_i are diffeomorphic to $(0,1)^{n_i}$, $n_i \leq n$ (see Proposition 2.9.10 of [25]). Let us denote these diffeomorphisms by $\phi_i : (0,1)^{n_i} \to S_i$. Since S is a finite union it suffices to prove that the m-dimensional Hausdorff measure of S_i is zero for $m > n$.

For each point $p \in S_i$, there is a neighbourhood N_p of p such that $\phi_i|_{N_p}$ is Lipschitz. Constructing such neighbourhoods for all $p \in S_i$, we obtain an open cover of S_i by the open sets $\{N_p\}_{p \in S_i}$ and since $\mathbb{R}^n$ is second countable there is a countable subcover $\{S_i \cap N_{p_j}\}_{j \in \mathbb{N}}$.

Finally, we just have to see that the Hausdorff measure of N_{p_j} is zero for all $j \in \mathbb{N}$. But $\phi_i(N_{p_j})$ is the image of a set of zero m-dimensional Hausdorff measure under a Lipschitz map and thus $\phi_i(N_{p_j})$ has zero m-dimensional Hausdorff measure as well. □

---

[19] Note that the definition of a representing set naturally generalizes to subsets $\mathcal{R} \subseteq H(\mathbb{C}^n)$.

[20] Theorem VI.2 also applies in this situation. See the remark after proof of Theorem VI.2 for more details.

Remark Note that this proof in particular shows that the n-dimensional Hausdorff measure of an n-dimensional semi-algebraic set does not vanish and hence it is a suitable measure for our purposes.

The set of measurement schemes always is a semi-algebraic subset S of a real affine space and the measure we choose for S is the m-dimensional Hausdorff measure where m is the dimension of S. If we say that almost all elements of an m-dimensional semi-algebraic set S has a certain property we mean that it fails to hold on a subset $A \subseteq S$ that has m-dimensional Hausdorff measure zero. We do this by showing that the algebraic dimension of A is smaller than m and applying Proposition A.1.

---

[1] Teiko Heinosaari, Luca Mazzarella, and Michael M Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318(2):355–374, 2013.

[2] Michael Kech, Péter Vrana, and Michael Wolf. The role of topology in quantum tomography. *Journal of Physics A: Mathematical and Theoretical*, 48(26):265303, 2015.

[3] R James Milgram. Immersing projective spaces. *The Annals of Mathematics*, 85(3):473–482, 1967.

[4] Karl Heinz Mayer. Elliptische differentialoperatoren und ganzzahligkeitssätze für charakteristische zahlen. *Topology*, 4(3):295–313, 1965.

[5] Stefan Weigert. Pauli problem for a spin of arbitrary length: A simple method to determine its wave function. *Physical Review A*, 45(11):7688, 1992.

[6] Jean-Pierre Amiet and Stefan Weigert. Reconstructing the density matrix of a spin s through stern-gerlach measurements: Ii. *Journal of Physics A: Mathematical and General*, 32(25):L269, 1999.

[7] Jean-Pierre Amiet and Stefan Weigert. Reconstructing the density matrix of a spin s through stern-gerlach measurements. *Journal of Physics A: Mathematical and General*, 31(31):L543, 1998.

[8] J Finkelstein. Pure-state informationally complete and "really" complete measurements. *Physical Review A*, 70(5):052107, 2004.

[9] Steven T Flammia, Andrew Silberfarb, and Carlton M Caves. Minimal informationally complete measurements for pure states. *Foundations of Physics*, 35(12):1985–2006, 2005.

[10] David Gross, Yi-Kai Liu, Steven T Flammia, Stephen Becker, and Jens Eisert. Quantum state tomography via compressed sensing. *Physical review letters*, 105(15):150401, 2010.

[11] Damien Mondragon and Vladislav Voroninski. Determination of all pure quantum states from a minimal number of observables. *arXiv preprint arXiv:1306.1214*, 2013.

[12] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. Tasks and premises in quantum state determination. *Journal of Physics A: Mathematical and Theoretical*, 47(7):075302, 2014.

[13] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. Expanding the principle of local distinguishability. *arXiv:1401.1481*, 2014.

[14] David Gross. Recovering low-rank matrices from few coefficients in any basis. *IEEE Trans. on Information Theory*, 57:1548–1566, 2011.

[15] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Applied and Computational Harmonic Analysis*, 20(3):345–356, 2006.

[16] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. *Applied and Computational Harmonic Analysis*, 2014.

[17] Bernhard G Bodmann and Nathaniel Hammen. Stable phase retrieval with low-redundancy frames. *Advances in Computational Mathematics*, pages 1–15, 2013.

[18] D. Gross, F. Krahmer, and R. Kueng. A partial derandomization of phaselift using spherical designs. *arXiv:1310.2267*, 2013.

[19] Philippe Jaming. Uniqueness results for the phase retrieval problem of fractional fourier transforms of variable order. *arXiv preprint arXiv:1009.3418*, 2010.

[20] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. How many orthonormal bases are needed to distinguish all pure quantum states? *arXiv preprint arXiv:1504.01590*, 2015.

[21] Richard Kueng, Holger Rauhut, and Ulrich Terstiege. Low rank matrix recovery from rank one measurements. *arXiv preprint arXiv:1410.6913*, 2014.

[22] Alexander S Holevo. *Probabilistic and statistical aspects of quantum theory*, volume 1. Springer, 2011.

[23] Paul Busch, Marian Grabowski, and Pekka Johannes Lahti. *Operational quantum physics*, volume 31. Springer, 1995.

[24] Frank W Warner. *Foundations of differentiable manifolds and Lie groups*, volume 94. Springer, 1971.

[25] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*. Springer, 1998.

[26] Markus Walgenbach. Lower bounds for the immersion dimension of homogeneous spaces. *Topology and its Applications*, 112(1):71–86, 2001.

[27] Frank Morgan. *Geometric measure theory: a beginner's guide*. Academic press, 2008.

Explicit Frames for Deterministic Phase Retrieval via PhaseLift

M. Kech August 24, 2016

The phase retrieval problem aims to reconstruct a signal $x \in \mathbb{C}^n$ up to a global phase factor from m intensity measurements, i.e., from measurements $|\langle x, v_1\rangle|^2, \dots, |\langle x, v_m\rangle|^2$, where $v_i \in \mathbb{C}^n$, $i = 1, \dots, m$. PhaseLift [1] is a reconstruction approach for the phase retrieval problem and essentially consists of two steps. First, as one has

$$|\langle x, v\rangle|^2 = \operatorname{tr}(xx^*vv^*),\ \forall x, v \in \mathbb{C}^n,$$

the phase retrieval problem is equivalent to recovering a positive rank one matrix from linear measurements. More precisely, given measurement vectors $v_i \in \mathbb{C}^n$, $i = 1, \dots, m$, such that the phase retrieval problem is well-posed, a signal $x \in \mathbb{C}^n$ can be recovered up to a global phase from the rank one matrix minimizing

$$\begin{aligned} &\text{minimize } \operatorname{rank} X \\ &\text{subject to } X \geq 0,\ \operatorname{tr}(Xv_iv_i^*) = \operatorname{tr}(xx^*v_iv_i^*),\ i = 1, \dots, m. \end{aligned}$$

As rank minimization is intractable in general [2], in a second step this optimization problem is relaxed to the semidefinite program (SDP)

$$\begin{aligned} &\text{minimize } \operatorname{tr} X \\ &\text{subject to } X \geq 0,\ \operatorname{tr}(Xv_iv_i^*) = \operatorname{tr}(xx^*v_iv_i^*),\ i = 1, \dots, m. \end{aligned} \tag{1}$$

1 Main Result

In this article, $5n - 6$ measurement vectors are constructed such that every signal $x \in \mathbb{C}^n$ can be recovered up to a global phase from their associated intensity measurements by solving the SDP (1).

For $k \in \{1, \dots, 2n-3\}$, choose $y_k \in \mathbb{R} \setminus \{0\}$ and set

$$v_k := \left(1, \quad y_k\, e^{\frac{i\pi}{2n}}, \quad y_k^2\, e^{2\frac{i\pi}{2n}}, \dots, \quad y_k^{n-1}\, e^{(n-1)\frac{i\pi}{2n}}\right)^t. \tag{2}$$

Theorem 1 (Frame for PhaseLift)**.** *Let*[1] $\mathcal{F} := \{e_0, \dots, e_{n-1}, v_1, \overline{v}_1, \dots, v_{2n-3}, \overline{v}_{2n-3}\}$ *and assume* $y_1 < y_2 < \ldots < y_{2n-3}$*. Then, for every* $x \in \mathbb{C}^n$*, the unique minimizer of*

$$\begin{aligned} &\textit{minimize } tr\, X \\ &\textit{subject to } X \geq 0,\ tr(Xvv^*) = tr(xx^*vv^*),\ \forall v \in \mathcal{F}, \end{aligned}$$

is given by xx^**.*

[1] The vectors $e_0, \dots, e_{n-1}$ denote the standard basis vectors of $\mathbb{C}^n$.

2 Stability

This approach can be generalized to the recovery of positive semidefinite matrices of rank at most r. Let $\mathcal{P}(\mathbb{C}^n) := \{X \in H(\mathbb{C}^n) | \, X \geq 0\}$ and $\mathcal{P}_r(\mathbb{C}^n) := \{X \in \mathcal{P}(\mathbb{C}^n) | \operatorname{rank} X \leq r\}$.

Definition 1. (r-complete.) A linear map $M : H(\mathcal{H}) \to \mathbb{R}^m$ is called r-complete iff $M(X) \neq M(X')$ holds for all $X \in \mathcal{P}_r(\mathbb{C}^n)$ and $X' \in \mathcal{P}(\mathbb{C}^n)$ with $X \neq X'$.

The linear map $M : H(\mathbb{C}^n) \to \mathbb{R}^{5n-6}$ induced by the measurement vectors given in Theorem 1 is 1-complete. Furthermore, in the article r-complete linear maps $M : H(\mathbb{C}^n) \to \mathbb{R}^{4r(n-r)+n-2r}$ are constructed for all $1 \leq r \leq n$.

Consider the SDP

$$\begin{aligned} &\text{minimize } \operatorname{tr}(Y) \\ &\text{subject to } Y \geq 0, \ \|M(Y) - b\| \leq \epsilon, \end{aligned} \tag{3}$$

where $\epsilon \geq 0$ is a constant representing the error scale.

The r-complete property comes with the following qualitative recovery result.

Theorem 2 (Recovery of low-rank positive matrices)**.** *Let $M : H(\mathcal{H}) \to \mathbb{R}^m$ be r-complete and let $\epsilon > 0$. There is a constant $C_M > 0$ independent of ϵ such that for all $X_r \in \mathcal{P}_r(\mathbb{C}^n)$ and $E \in H(\mathbb{C}^n)$ with $\|M(E)\|_2 \leq \epsilon$, any minimizer Y of (3) for $b = M(X_r + E)$ satisfies*

$$\|Y - X_r\|_{HS} \leq C_M \epsilon.$$

References

[1] Emmanuel J Candes, Thomas Strohmer, and Vladislav Voroninski. Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming. *Communications on Pure and Applied Mathematics*, 66(8):1241–1274, 2013.

[2] Balas Kausik Natarajan. Sparse approximate solutions to linear systems. *SIAM journal on computing*, 24(2):227–234, 1995.

Explicit Frames for Deterministic Phase Retrieval via PhaseLift

Michael Kech[1,*]

[1]*Department of Mathematics, Technische Universität München, 85748 Garching, Germany*

(Dated: July 13, 2016)

We explicitly give a frame of cardinality $5n-6$ such that every signal in $\mathbb{C}^n$ can be recovered up to a phase from its associated intensity measurements via the PhaseLift approach. Furthermore, we give explicit linear measurements with $4r(n-r)+n-2r$ outcomes that enable the recovery of every positive semidefinite $n \times n$ matrix of rank at most r.

Keywords: phase retrieval, PhaseLift, low-rank matrix recovery, quantum state tomography

Contents

I. INTRODUCTION AND MAIN RESULT

Phase Retrieval is the task of reconstructing a signal $x \in \mathbb{C}^n$ up to a phase from intensity measurements.

In [1] it was shown that $m \geq 4n-2$ generic intensity measurements suffice to discriminate any two signals in $\mathbb{C}^n$ up to a phase. With a similar approach this result was slightly improved to $m \geq 4n-4$ in [2] [1]. The bound $m \geq 4n-4$ is known to be close to optimal. More precisely, by relating phase retrieval to the problem of embedding complex projective space in Euclidean space, it was shown in [6] that, up to terms at most logarithmic in n, $m \geq 4n-4$ intensity measurements are necessary to discriminate any two signals in

*Electronic address: kech@ma.tum.de

[1] In the context of pure state tomography, [3–5] show that the $4n-4$ bound also holds for von Neumann measurements. In addition similar bounds for the recovery of low-rank matrices with constrained measurements are provided in [3].

$\mathbb{C}^n$ up to a phase. However, [1, 2] do not provide a tractable recovery scheme. A result indicating that some redundancy is needed in order to allow for computationally efficient phase retrieval is given in [7].

There have been several approaches that do provide recovery schemes [8–10], in the present paper however we focus on the approach of [11] known as PhaseLift. Their approach consists of two steps: First, phase retrieval is lifted to the problem of recovering rank one Hermitian matrices from linear measurements. Secondly, by means of a convex relaxation, the recovery problem is formulated as a trace norm minimization over a spectrahedron. The authors of [11] then prove that $\mathcal{O}(n)$ intensity measurements suffice to recover a signal modulo phase with high probability by solving the relaxed optimization problem. Furthermore, stability guarantees for the recovery were established in [12, 13]. While these convex relaxations are in principal tractable, solving them becomes computationally expensive with increasing signal dimension [14].

However, [11–13] still leave room for improvement. For example, by working with Gaussian random vectors additional structure that might facilitate the use of PhaseLift is not incorporated and also from a practical point of view Gaussian random vectors might not be desirable. Recently, it was shown that a partial derandomization of PhaseLift can be achieved by using spherical designs [15, 16]. The purpose of the present paper is similar. However, rather than drawing the measurements from a smaller, possibly better structured set, we aim for finding explicit measurements that allow for phase retrieval via PhaseLift. Another deterministic approach to the phase retrieval problem was introduced in [17]. They improved their results in [18], providing recovery algorithms together with explicit error bounds for phase retrieval with $6n-3$ frame vectors.

Our contribution is the following: We explicitly give $5n-6$ intensity measurements from which every signal in $\mathbb{C}^n$ can be reconstructed up to a phase using PhaseLift. More precisely, for $k \in \{1,\dots,2n-3\}$ let

$$v_k := \left(1,\ x_k\, e^{\frac{i\pi}{2n}},\ x_k^2\, e^{2\frac{i\pi}{2n}},\ \dots,\ x_k^{n-1}\, e^{(n-1)\frac{i\pi}{2n}}\right)^t,\ x_k \in \mathbb{R}\setminus\{0\}. \tag{1}$$

Furthermore denote by $\{e_i\}_{i\in\{0,\dots,n-1\}}$ the standard orthonormal basis of $\mathbb{C}^n$.

Theorem I.1. *If $x_1 < x_2 < \ldots < x_{2n-3}$, then every signal $x \in \mathbb{C}^n$ can be reconstructed up to a phase from the $5n-6$ intensities*

$$\{|\langle e_0,x\rangle|^2,\dots,|\langle e_{n-1},x\rangle|^2,|\langle v_1,x\rangle|^2,|\langle \overline{v}_1,x\rangle|^2,\dots,|\langle v_{2n-3},x\rangle|^2,|\langle \overline{v}_{2n-3},x\rangle|^2\}$$

via PhaseLift.

This result is stated more carefully in Section III as Corollary III.2. Its proof relies on the results of [19].

Let us highlight three features of this result:

1. To our knowledge the $5n-6$ is the smallest number of intensity measurements that allow for a uniform and computationally tractable recovery.

2. Results based on random intensity measurements typically guarantee that the recovery succeeds with high probability if the number of measurements exceeds a given

threshold which is usually determined up to a multiplicative constant. As opposed to this, Theorem I.1 comes with two advantages that might be desirable from a practical point of view: First, the recovery is not just guaranteed to succeed with high probability but indeed works deterministically. Secondly, since the measurements are given explicitly there is no need for finding a suitable value for the threshold.

3. Theorem I.1 merely requires $5n - 6$ intensity measurements. This illustrates that n additional measurements as compared to the nearly optimal bound of [1] suffice to render PhaseLift feasible.

The approach we take originates from low-rank matrix recovery [20–24] and indeed the previous results can be generalised to this setting: In Section III, we give an explicit family of linear measurements with $4r(n-r)+n-2r$ outcomes from which every positive $n \times n$ matrix of rank at most r can be recovered by means of a semidefinite program. This strongly relies on the construction of the null spaces of such measurements given in [19]. Our contribution is to explicitly characterize the orthogonal complements of these null spaces leading to the proofs of our main results.

As stability was not mentioned in the abstract, I did not change this part. I changed the last section in the introduction to: Finally we also prove a weak stability result in Section IV, showing that the reconstruction error is linear in the error scale. As we do not know how to estimate the constant of proportionality appearing in the stability bound, this result is not of practical relevance, but might give a roadmap for proving stability in the future. However, we provide some numerical results that might indicate the constant's qualitative behaviour.

II. PRELIMINARIES

Let us first fix some notation. By $M(n,q)$ ($M(n,q,\mathbb{R})$) we denote the set of complex (real) $n \times q$ matrices. The transpose (conjugate transpose) of a matrix $A \in M(n,q)$ is denoted by A^t (A^*). For $i \in \{0,\dots,n-1\}$, $j \in \{0,\dots,q-1\}$, we denote the entry in the i-th row and j-th column of a matrix $A \in M(n,q)$ by A_{ij} [2]. By $H(n)$ we denote the real vector space of Hermitian $n \times n$ matrices. We equip $H(n)$ with the Hilbert-Schmidt inner product and $\|\cdot\|_2$ denotes the Frobenius norm. By $\mathcal{S}^n$ we denote the set of positive semidefinite $n \times n$ matrices and by $\mathcal{S}^n_r \subseteq \mathcal{S}^n$ we denote the subset of positive semidefinite matrices of rank at most r. In the following we assume that $r \in \{1,\dots,\lceil n/2 \rceil - 1\}$ [3]. The set of linear maps $M : H(n) \to \mathbb{R}^m$ is denoted by $\mathcal{M}(m)$.

Definition II.1. *(m-measurement.) An m-measurement is an element of $\mathcal{M}(m)$.*

In the following we denote an m-measurement simply by measurement if we do not want to specify m.

---

[2] Note that the indices we use to label matrices begin with 0, not with 1.

[3] $\lceil k \rceil :=$ the smallest integer i such that $i \geq k$.

Remark For each m-measurement M there exists a unique $G := (G_1, \ldots, G_m) \in H(n)^m$ such that

$$M(X) = \big(\mathrm{tr}(G_1 X), \ldots, \mathrm{tr}(G_m X)\big)$$

for all $X \in H(n)$. By M_G we denote the m-measurement associated in this way to an $G \in H(n)^m$. In the following we sometimes use this identification to speak of elements $G \in H(n)^m$ as m-measurements.

Definition II.2. *(r-complete.) A measurement M is called r-complete iff $M(X) \neq M(X')$ for all $X \in \mathcal{S}_r^n$ and $X' \in \mathcal{S}^n$ with $X \neq X'$. A tuple $G \in H(n)^m$ is called r-complete iff M_G is r-complete.*

Given a measurement M and a measurement outcome $b = M(X),\ X \in \mathcal{S}_r^n$, consider the following well-known semi-definite program [20, 22, 23] [4]

$$\begin{aligned} &\text{minimize } \mathrm{tr}(Y) \\ &\text{subject to } Y \geq 0,\ M(Y) = b. \end{aligned} \tag{2}$$

The significance of the r-complete property is due to the following observation:

Proposition II.1. *Let M be an r-complete measurement and let $X \in \mathcal{S}_r^n$. If $b = M(X)$, then X is the unique minimizer of the semidefinite program* (2).

Proof. Let $X \in \mathcal{S}_r(\mathbb{C}^n)$ be a Hermitian matrix of rank at most r and let M be an r-complete measurement. Then, X is the unique feasible point of the spectrahedron

$$\{Y \in H(n) : Y \geq 0,\ M(Y) = M(X)\}. \tag{3}$$

This follows immediately from $\{Y \in H(n) : Y \geq 0,\ M(Y) = M(X)\} = \{Y \in \mathcal{S}^n : M(Y) = M(X)\}$ and the definition of r-complete. □

Remark Note that if $\mathbb{1} \in \mathrm{Range}(M^*)$, the r-complete property also is necessary for a deterministic reconstruction via the semidefinite program (2).

This shows that for an r-complete measurement the semidefinite program (2) reduces to a feasibility problem.

Finally, let us state the observation of [19, 25] which gives a useful characterization of the r-complete property:

Proposition II.2. *A measurement M is r-complete if and only if every nonzero $X \in Ker(M)$ has at least $r + 1$ positive eigenvalues.*

[4] This is a convex relaxation of the rank minimization problem.

Proof. Consider the set $\Delta := \{Y - Z : Y \in \mathcal{S}_r^n,\ Z \in \mathcal{S}^n\}$ and note that every $X \in \Delta$ has at most r positive eigenvalues. Furthermore, note that a measurement M is r-complete if and only if $\Delta \cap \mathrm{Ker}(M) \setminus \{0\} = \emptyset$.

Now assume that every $X \in \mathrm{Ker}(M) \setminus \{0\}$ has at least $r+1$ positive eigenvalues. Since every $Y \in \Delta$ has at most r positive eigenvalues we find $Y \notin \mathrm{Ker}(M) \setminus \{0\}$, i.e. $\Delta \cap \mathrm{Ker}(M) \setminus \{0\} = \emptyset$.

Conversely, assume that M is r-complete. Δ clearly contains all matrices with at most r positive eigenvalues and hence $\mathrm{Ker}(M) \setminus \{0\}$ cannot contain an element with r or less positive eigenvalues.

□

Remark If every nonzero $X \in \mathrm{Ker}(M)$ has at least $r+1$ positive eigenvalues, then every nonzero $X \in \mathrm{Ker}(M)$ also has at least $r+1$ negative eigenvalues since $X \in \mathrm{Ker}(M)$ implies $-X \in \mathrm{Ker}(M)$.

III. RECONSTRUCTION OF LOW-RANK POSITIVE MATRICES

Our approach relies on [19] where a method to construct the null spaces of r-complete m-measurements for $m = 4r(n-r) + n - 2r$ is provided. Their construction is based on the ideas of [26], details can be found in Appendix A of [19].

First, we focus on the phase retrieval problem.

Theorem III.1. *Let*

$$G := \left(e_0 e_0^*, \ldots, e_{n-1} e_{n-1}^*, \frac{v_1 v_1^*}{\|v_1 v_1^*\|_2}, \frac{\overline{v}_1 \overline{v}_1^*}{\|\overline{v}_1 \overline{v}_1^*\|_2}, \ldots, \frac{v_{2n-3} v_{2n-3}^*}{\|v_{2n-3} v_{2n-3}^*\|_2}, \frac{\overline{v}_{2n-3} \overline{v}_{2n-3}^*}{\|\overline{v}_{2n-3} \overline{v}_{2n-3}^*\|_2} \right),$$

where the v_i are defined in Equation (1)*. If $x_1 < x_2 < \ldots < x_{2n-3}$, then the measurement M_G is* 1*-complete.*

The proof of this theorem can be found in Section V.

Remark From the proof of this result it is easily seen that the kernel of M_G is independent of the choice of the x_i. Thus, for the purpose of robustness, the x_i should be chosen such that the smallest singular value of M_G is maximized.

Let us next state Theorem I.1 in a more precise way.

Corollary III.2. *(Phase Retrieval via PhaseLift.) Let M be a measurement given by Theorem III.1 and let $x \in \mathbb{C}^n$. If $b = M(xx^*)$, then xx^* is the unique minimizer of the semidefinite program* (2)*.*

By Proposition II.1, this is an immediate consequence of Theorem III.1.

Let us next focus on the recovery of low-rank positive matrices. This, however, requires some further definitions: First, let

$$C_r^n := \{X \in H(n) : \mathrm{tr}(X e_i e_j^*) = 0,\ 2r - 1 \leq i + j \leq 2(n-r) - 1,\ i \neq j, \}. \tag{4}$$

E.g. $C_1^n \subseteq H(n)$ is the subspace of $n \times n$ diagonal matrices and C_3^7 is the subspace of $H(7)$ of the from

$$\begin{pmatrix} * & * & * & * & * & 0 & 0 \\ * & * & * & * & 0 & 0 & 0 \\ * & * & * & 0 & 0 & 0 & * \\ * & * & 0 & * & 0 & * & * \\ * & 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & * & * & * & * & * \end{pmatrix}.$$

For $x \in \mathbb{R} \setminus \{0\}$, $k \in \{2r-1, \ldots, 2(n-r)-1\}$, define the Hermitian matrices $R_k(x), I_k(x) \in (C_r^n)^\perp$ by [5]

$$(R_k(x))_{jl} := \delta_{j+l,k} x^j, \ j,l \in \{0,\ldots,n-1\}, \ j > l,$$
$$(I_k(x))_{jl} := i\delta_{j+l,k} x^j, \ j,l \in \{0,\ldots,n-1\}, \ j > l,$$

where $\delta_{i,j}$ denotes the Kronecker delta. E.g. for $n = 5$, $r = 2$ these are

$$R_3(x) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & x & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, I_3(x) = \begin{pmatrix} 0 & 0 & 0 & i & 0 \\ 0 & 0 & ix & 0 & 0 \\ 0 & -ix & 0 & 0 & 0 \\ -i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, R_4(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & x & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, I_4(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & i \\ 0 & 0 & 0 & ix & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -ix & 0 & 0 & 0 \\ -i & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$R_5(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}, I_5(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & i \\ 0 & 0 & 0 & ix & 0 \\ 0 & 0 & -ix & 0 & 0 \\ 0 & -i & 0 & 0 & 0 \end{pmatrix}.$$

Theorem III.3. *Let G_0 be a basis of C_r^n and let $x_1, x_2, \ldots, x_r \in \mathbb{R} \setminus \{0\}$ with $x_1 < x_2 < \ldots < x_r$. For $k \in \{2r-1, \ldots, 2(n-r)-1\}$ define*

$$G_k := (I_k(x_1), R_k(x_1), \ldots, I_k(x_r), R_k(x_r)).$$

and let $G := G_0 \cup G_{2r-1} \cup \cdots \cup G_{2(n-r)-1}$ [6]. Then the measurement M_G is r-complete and $|G| = 4r(n-r) + n - 2r$.

Remark If an m-measurement is injective when restricted to $\mathcal{S}_r^n$, it was shown in [6, 27] that, up to terms at most logarithmic in n, we have $m \geq 4r(n-r)$. Furthermore, in [3, 6] it was shown that there indeed exist injective m-measurements for $m = 4r(n-r)$. Thus, it might be worth noting that the measurements given by Theorem III.3 solely require $n-2r$ additional measurement outcomes as compared to the nearly optimal bound $4r(n-r)$.

Finally, by Proposition II.1, the measurements given by Theorem III.3 allow for the recovery of low-rank positive matrices.

Corollary III.4. *(Recovery of low-rank positive matrices.) Let M be a measurement given by Theorem III.3 and let $X \in \mathcal{S}_r^n$. If $b = M(X)$, then X is the unique minimizer of the semidefinite program* (2).

---

[5] As $R_k(x), I_k(x) \in (C_r^n)^\perp$ both have vanishing diagonal and since they are hermitian, it suffices to define all elements above the diagonal.

[6] For tuples of Hermitian matrices $X := (X_1, \ldots, X_i) \in H(n)^i$, $Y := (Y_1, \ldots, Y_j) \in H(n)^j$ we define their union $X \cup Y$ to be the tuple $X \cup Y := (X_1, \ldots, X_i, Y_1, \ldots, Y_j) \in H(n)^{i+j}$.

IV. STABILITY

In this section we discuss the stability of r-complete measurements.

Assume there is an error term $E \in H(n)$ that perturbs the matrix $X_r \in \mathcal{S}_r^n$ we intend to recover to the matrix $X = X_r + E$. Measuring with an r-complete measurement M yields the perturbed outcome $b = M(X)$. Clearly, the matrix X_r cannot always be perfectly recovered from the outcome b, however, if $\|M(E)\|_2$ is small, there is a recovery procedure that yields a matrix close to X_r. For that purpose, consider the following well-known optimization problem

$$\begin{aligned} &\text{minimize } \operatorname{tr}(Y) \\ &\text{subject to } Y \geq 0,\ \|M(Y) - b\|_2 \leq \epsilon \end{aligned} \tag{5}$$

where $\epsilon \geq 0$ is a constant representing the error scale.

Theorem IV.1. *(Stable recovery of low-rank positive matrices.) Let M be an r-complete measurement and let $\epsilon > 0$. There is a constant $C_M > 0$ independent of ϵ such that for all $X_r \in \mathcal{S}_r^n$ and $E \in H(n)$ with $\|M(E)\|_2 \leq \epsilon$, any minimizer Y of (5) for $b = M(X_r + E)$ satisfies*

$$\|Y - X_r\|_2 \leq C_M \epsilon.$$

Remark In the proof of this theorem we show that $C_M \leq \frac{2}{\sigma_{\min}}(1 + \frac{1}{\kappa})$ where σ_{min} is the smallest singular value of M and $\kappa := -\max_{Z \in \operatorname{Ker}(M), \|Z\|_2 = 1} \lambda_{n-r}(Z)$ [7]. However we do not know how to compute κ for a given r-complete measurement M and hence we cannot make this bound more explicit.

The proof of this theorem can be found in Section V. In order for this result to be a practical stability guarantee, one would have to estimate the constant C_M. At this point we do not know how this can be achieved. In order to indicate the magnitude of the constant C_M, let us next present some numerical results. For this purpose consider the tuple

$$G_n := \left(e_0 e_0^*, \ldots, e_{n-1} e_{n-1}^*, \frac{I_1(1)}{\|I_1(1)\|_2}, \frac{R_1(1)}{\|R_1(1)\|_2}, \ldots, \frac{I_{2n-3}(1)}{\|I_{2n-3}(1)\|_2}, \frac{R_{2n-3}(1)}{\|R_{2n-3}(1)\|_2} \right)$$

and note that by Theorem III.3 the associated measurement M_{G_n} is 1-complete. Figure 1 presents numerical results that might indicate the scaling of $C_{M_{G_n}}$ for the sequence of measurements $(M_{G_n})_{n \in \mathbb{N}}$.

Just like in [12], this recovery scheme can also be used for the phase retrieval problem. For a Hermitian matrix $A \in H(n)$, we denote by $\operatorname{Eig}(A) \in \mathbb{R}^n$ the tuple of eigenvalues of A ordered decreasingly together with their multiplicities. Furthermore, we define $\lambda_i(A) := \operatorname{Eig}(A)_{i-1},\ i \in \{1, \ldots, n\}$.

[7] λ_{n-r} is defined later this section.

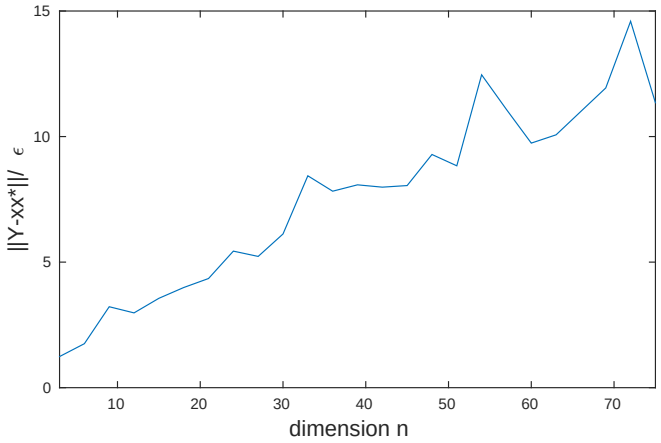

FIG. 1: For each $n \in \{3, 6, \ldots, 75\}$ we choose uniformly at random a normalized vector $x \in \mathbb{C}^n$ and an error term $f \in \mathbb{R}^{5n-6}$ with $\|f\|_2 \leq \epsilon := 10^{-3}$. Then we run the program (5) with the outcome $b = M_{G_n}(xx^*) + f$. The figure shows the maximum value of $\|Y - xx^*\|_2/\epsilon$ for 2200 repetitions where Y is the minimizer of (5).

Proposition IV.2. *(Stability for Phase Retrieval.) Let $X = xx^* + E$, where $x \in \mathbb{C}^n$ is the signal and $E \in H(n)$ is an error term. Let M be a 1-complete measurement and let $\epsilon \geq \|M(E)\|_2$. Furthermore, let Y be any minimizer of the optimization problem (5) for $b = M(X)$ and set $\hat{x} := \sqrt{\lambda_1(Y)}x'$ where $x' \in S^{n-1}$ is an eigenvector of Y with eigenvalue $\lambda_1(Y)$. Then*

$$\|xx^* - \hat{x}\hat{x}^*\|_2 \leq 2C_M\epsilon,$$

where C_M is the constant given by Theorem IV.1. Furthermore, for some $\varphi \in [0, 2\pi)$ we have

$$\|x - e^{i\varphi}\hat{x}\|_2 \leq \frac{2\sqrt{2}C_M}{\|x\|_2}\epsilon.$$

This result follows from Theorem IV.1 by a straightforward computation. The proof is given in Section V.

Remark The proofs of V.5 shows that the above stability results also hold true the following recovery scheme:

$$\begin{aligned} &\text{minimize } \|M(Y) - b\|_2 \\ &\text{subject to } Y \geq 0, \end{aligned} \tag{6}$$

where M is r-complete and $b = M(X_r + E)$, $X_r \in \mathcal{S}_r^n$.

V. TECHNICAL APPENDIX

Let us first introduce some notation we use throughout this section. Let $A \in M(n,q)$, $i \in \{0,\dots,n-1\}$, $j \in \{0,\dots,q-1\}$. By $A_{,i}$ we denote the $(n-1)\times q$ matrix obtained from A by deleting the i-th row and by $A^{,j}$ we denote the $n \times (q-1)$ matrix obtained from A by deleting the j-th column. By $A\{i\}$ we denote the i-th row of A and by $A[j]$ we denote the j-th column of A. Furthermore, for $k \in \{0,\dots,n+q-2\}$, we denote the k-th anti-diagonal of A by $A(k)$, i.e. $A(k) := (A_{ij})_{i+j=k}$ [8].

A. Proof of Theorem III.3

Since Theorem III.1 is obtained by manipulating the measurements obtained from Theorem III.3 we begin by proving the latter. The construction we give in the following yields a more general class of r-complete measurements than the ones given by Theorem III.3 and it strongly relies on the notion of totally non-singular matrices.

Definition V.1. *(Totally non-singular.) A matrix $A \in M(n,q)$ is called totally non-singular if A has no vanishing minor.*

The following lemma is a central ingredient for the construction given in the following.

Lemma V.1. *Let $q \in \{1,\dots,n-1\}$ and let $A \in M(n,q)$ be totally non-singular. Then, there exists a totally non-singular matrix $B \in M(n,n-q)$ such that $A^*B = 0$.*

Proof. We give a proof by induction in the dimension n for q fixed.

Base case. Let us begin with the base case $n = q+1$. Note that for a given $A \in M(q+1,q)$ there always exists a nonzero matrix (actually just a vector) $B \in M(q+1,1)$ such that $A^*B = 0$, in particular if A is totally non-singular.

Since B exists, it is enough to prove that if A is totally non-singular B is totally non-singular as well: Assume for a contradiction that B is not totally non-singular, i.e. that B has a vanishing entry. By permuting rows we can assume A and B to be of the form

$$A = \begin{pmatrix} F \\ D \end{pmatrix}, \quad B = \begin{pmatrix} 0 \\ E \end{pmatrix}$$

for some matrices $F \in M(1,q)$, $D \in M(q,q)$ and $E \in M(q,1)$. But then

$$A^*B = F^*0 + D^*E = D^*E = 0.$$

In particular this implies that the $q \times q$ submatrix D of A is singular, contradicting the fact that A is totally non-singular by assumption.

Induction step. Assume the claim holds for an $n > q$ and let $A \in M(n+1,q)$ be totally non-singular. Note that for each $i \in \{0,\dots,n\}$, the $n \times q$ matrix $A_{,i}$ is totally non-singular since A is totally non-singular. Thus, by the induction hypothesis, we can find for

[8] The ordering is such that the matrix element with smaller i comes first.

each $i \in \{0,\dots,n\}$ a totally non-singular matrix $C_i \in M(n, n-q)$ such that $A^*_{,i}C_i = 0$. For $i \in \{0,\dots,n\}, j \in \{0,\dots,n-q\}$ let $C(i,j) \in M(n+1, n+1-q)$ be the matrix with $C(i,j)^{,j}_{,i} = C_i$ and 0 else. Then, for all $i \in \{0,\dots,n\}, j \in \{0,\dots,n-q\}$, $C(i,j)^{,j}_{,i}$ is totally non-singular, $C(i,j)[j] = 0$ and $A^*C(i,j) = 0$ by construction.

Step 1. First, for each $i \in \{0,\dots,n\}$, we deform $C(i,0)$ into a matrix $\tilde{C}(i,0) \in M(n+1, n+1-q)$ with the following properties:

1. $A^*\tilde{C}(i,0) = 0$,
2. $\tilde{C}(i,0)^{,0}_{,i}$ is totally non-singular,
3. All $(n+1-q) \times (n+1-q)$ minors of $\tilde{C}(i,0)_{,i}$ are nonzero.

Let $i \in \{0,\dots,n\}$. For $\sigma := (k_0,\dots,k_{n-q}) \in \Sigma := \{(l_0,\dots,l_{n-q}) : 0 \le l_0 < \dots < l_{n-q} \le n-1\}$ define the projection $P_\sigma : M(n+1, n+1-q) \to M(n+1-q, n+1-q)$ by $P_\sigma(X)\{j\} := (X_{,i})\{k_j\}$ for all $X \in M(n+1, n+1-q), j \in \{0,\dots,n-q\}$. Now let $\sigma \in \Sigma$, and set $E_\sigma := P_\sigma(C(i,0))$. By permuting rows we can assume A and $C(i,0)$ to be of the form

$$A = \begin{pmatrix} F \\ D \end{pmatrix}, \quad C(i,0) = \begin{pmatrix} E_\sigma \\ F_\sigma \end{pmatrix} \tag{7}$$

for some matrices $F \in M(n+1-q, q)$, $D \in M(q,q)$ and $F_\sigma \in M(q, n+1-q)$.

Next, we show that there is a vector $u_\sigma = \begin{pmatrix} v_\sigma \\ w_\sigma \end{pmatrix}$ [9], where $v_\sigma \in \mathbb{C}^{n+1-q}$, $w_\sigma \in \mathbb{C}^q$, such that $A^*u_\sigma = 0$ and $\det(E_\sigma + P_\sigma(u_\sigma e_0^*)) = \det(E_\sigma + v_\sigma e_0^*) \neq 0$: Since C_i is totally non-singular, E_σ has rank $n-q$. Thus we can find a vector $v_\sigma \in \mathbb{C}^{n+1-q}$ such that $\det(E_\sigma + v_\sigma e_0^*) \neq 0$ [10]. Finally, we just have to ensure that $A^*u_\sigma = 0$. Since D is totally non-singular there is a vector $w_\sigma \in \mathbb{C}^q$ such that $D^*w_\sigma = -F^*v_\sigma$ and this gives $A^*\begin{pmatrix} v_\sigma \\ w_\sigma \end{pmatrix} = F^*v_\sigma + D^*w_\sigma = 0$. Repeating this construction, we can find a collection of vectors $\{u_\sigma\}_{\sigma\in\Sigma} \subseteq \mathbb{C}^{n+1}$ such that for all $\sigma \in \Sigma$ we have $A^*u_\sigma = 0$ and $\det\big(P_\sigma(C(i,0) + u_\sigma e_0^*)\big) \neq 0$.

Next, for distinct $\sigma_1, \sigma_2 \in \Sigma$, define the mapping $K(\lambda) := C(i,0) + u_{\sigma_1}e_0^* + \lambda u_{\sigma_2}e_0^*$, $\lambda \in \mathbb{C}$ and note that by construction $A^*K(\lambda) = 0$ for all $\lambda \in \mathbb{C}$. Note that by construction $K(\lambda)^{,0}_{,i} = C_i$ is totally non-singular for all λ. Furthermore, the $(n+1-q) \times (n+1-q)$ minors $\det\big(P_{\sigma_1}(K(\lambda))\big)$ and $\det\big(P_{\sigma_2}(K(\lambda))\big)$ can be considered as polynomials in λ. The polynomial equations $\det\big(P_{\sigma_1}(K(\lambda))\big) = 0$ and $\det\big(P_{\sigma_2}(K(\lambda))\big) = 0$ are non-trivial: For $\lambda = 0$ we have $\det\big(P_{\sigma_1}(K(0))\big) = \det\big(P_{\sigma_1}(C(i,0) + u_{\sigma_1}e_0^*)\big) \neq 0$ by construction. For λ large one can consider $\frac{1}{\lambda}u_{\sigma_1}e_0^*$ as a small perturbation to $u_{\sigma_2}e_0^*$. Thus, using linearity of

[9] The direct sum decomposition of u_σ is with respect to the decomosition given by Equation (7), i.e. $A^*u_\sigma = F^*v_\sigma + D^*w_\sigma$.

[10] Note that $E_\sigma[0] = 0$ by construction of $C(i,0)$.

the determinant in the 0-th column, we conclude that

$$\begin{aligned}\det\big(P_{\sigma_2}(K(\lambda))\big) &= \det\big(P_{\sigma_2}(C(i,0)+u_{\sigma_1}e_0^*+\lambda u_{\sigma_2}e_0^*)\big)\\ &= \lambda\cdot\det\big(P_{\sigma_2}(C(i,0)+u_{\sigma_2}e_0^*)+\frac{1}{\lambda}P_{\sigma_2}(u_{\sigma_1}e_0^*)\big)\neq 0\end{aligned}$$

for large enough λ by the continuity of the determinant and the fact that $\det\big(P_{\sigma_2}(C(i,0)+u_{\sigma_2}e_0^*)\big)\neq 0$ by construction. A non-trivial polynomial equation in one variable just has a finite set of solutions and hence the set

$$\begin{aligned}&\{\lambda\in\mathbb{C}:\det\big(P_{\sigma_1}(K(\lambda))\big)=0\vee\det\big(P_{\sigma_2}(K(\lambda))\big)=0\}\\ =\{\lambda\in\mathbb{C}:\det\big(P_{\sigma_1}(K(\lambda))\big)=0\}&\cup\{\lambda\in\mathbb{C}:\det\big(P_{\sigma_2}(K(\lambda))\big)=0\}\end{aligned}$$

is finite. In particular there is an $a_{\sigma_2}\in\mathbb{C}$ such that $\det\big(P_{\sigma_1}(K(a_{\sigma_2}))\big)\neq 0$ and $\det\big(P_{\sigma_2}(K(a_{\sigma_2}))\big)\neq 0$ [11]. Applying the same argument to $L(\lambda):=C(i,0)+u_{\sigma_1}e_0^*+a_{\sigma_2}u_{\sigma_2}e_0^*+\lambda u_{\sigma_3}e_0^*$, $\lambda\in\mathbb{C}$, where $\sigma_3\in\Sigma$ is distinct from σ_1,σ_2, yields an $a_{\sigma_3}\in\mathbb{C}$ such that $\det\big(P_{\sigma_1}(L(a_{\sigma_3}))\big)\neq 0$, $\det\big(P_{\sigma_2}(L(a_{\sigma_3}))\big)\neq 0$ and $\det\big(P_{\sigma_3}(L(a_{\sigma_3}))\big)\neq 0$ [12]. Finally, since $|\Sigma|$ is finite, we can inductively apply the argument to obtain a matrix $\tilde{C}(i,0)=C(i,0)+u_{\sigma_1}e_0^*+\sum_{\sigma\in\Sigma,\sigma\neq\sigma_1}a_\sigma u_\sigma e_0^*$ with the desired properties.

Step 2. Secondly, we construct for each $i\in\{0,\dots,n\}$ a matrix $D_i\in M(n+1,q)$ with the following properties:

1. $A^*D_i=0$.
2. $(D_i)_{,i}$ is totally non-singular.

Let $i\in\{0,\dots,n\}$. Let $D_i(\lambda_1,\dots,\lambda_{n-q}):=\tilde{C}(i,0)+\sum_{j=1}^{n-q}\lambda_j C(i,j)$ where $\lambda_j\in\mathbb{C}$, $j\in\{1,\dots,n-q\}$, and note that by construction we have $A^*D_i(\lambda_1,\dots,\lambda_{n-q})=0$ for all $\lambda_1,\dots,\lambda_{n-q}\in\mathbb{C}$. By choosing $(\lambda_1,\dots,\lambda_{n-q})$ appropriately one can make sure that $(D_i(\lambda_1,\dots,\lambda_{n-q}))_{,i}$ is totally non-singular: First let $G(\lambda):=\tilde{C}(i,0)+\lambda C(i,1)$, $\lambda\in\mathbb{C}$. Just like in Step 1, the minors of $G(\lambda)^{,0}_{,i}$ and $G(\lambda)^{,1}_{,i}$ together with the $(n+1-q)\times(n+1-q)$ minors of $G(\lambda)_{,i}$ yield a finite set of polynomial equations in λ. All of these polynomial equations are non-trivial: For $\lambda=0$ none of the minors of $G(0)^{,0}_{,i}=C_i$ and none of the $(n+1-q)\times(n+1-q)$ minors of $G(0)_{,i}=\tilde{C}(i,0)_{,i}$ vanish by construction of $\tilde{C}(i,0)$. For large λ one can consider $\frac{1}{\lambda}\tilde{C}(i,0)$ as a small perturbation to $C(i,1)$. Hence, for large enough λ, none of the minors of $\frac{1}{\lambda}G(\lambda)^{,1}_{,i}$ vanishes by the fact that $C(i,1)^{,1}_{,i}=C_i$ is totally non-singular by construction and the continuity of the minors. Thus, just like in Step 1, we conclude that there are just finitely many values of λ for which any of these polynomials vanishes. In particular there is an $\lambda_1\in\mathbb{C}$ such that both $G(\lambda_1)^{,0}_{,i}$ and $G(\lambda_1)^{,1}_{,i}$ are totally non-singular and all $(n+1-q)\times(n+1-q)$ minors of $G(\lambda_1)_{,i}$ are nonzero. Applying the same argument to $H(\lambda):=\tilde{C}(i,0)+\lambda_1C(i,1)+\lambda C(i,2)$, $\lambda\in\mathbb{C}$, yields an $\lambda_2\in\mathbb{C}$ such that $H(\lambda_2)^{,0}_{,i}$, $H(\lambda_2)^{,1}_{,i}$ and $H(\lambda_2)^{,2}_{,i}$ are totally non-singular and all $(n+1-q)\times(n+1-q)$

[11] In fact this holds for almost all $a_{\sigma_2}\in\mathbb{C}$.

[12] Also in this case we obtain a finite set of non-trivial polynomial equations in λ and thus the argument given before can be applied to find a_{σ_3}.

minors of $H(\lambda_2)_{,i}$ are nonzero. Choosing the values for λ_j, $j \in \{1, \dots, n-q\}$, inductively in this fashion finally yields a matrix D_i with the desired properties.

Step 3. To complete the induction step we choose by a similar argument as in Step 1 and Step 2 before parameters $\gamma_j \in \mathbb{C}$, $j \in \{1, \dots, n\}$, in $B := D_0 + \sum_{j=1}^{n} \gamma_j D_j$ such that $B_{,i}$ is totally non-singular for each $i \in \{0, \dots, n\}$, i.e. such that B is totally non-singular: First define $I(\lambda) := D_0 + \lambda D_1$, $\lambda \in \mathbb{C}$. Clearly $I(0)_{,0} = (D_0)_{,0}$ is totally non-singular by construction of D_0. Furthermore, for large λ , $\frac{1}{\lambda} D_0$ can be considered as a small perturbation to D_1. Thus, for λ large enough, $\frac{1}{\lambda} I(\lambda)_{,1}$ is totally non-singular by construction of D_1 and the continuity of the minors. Hence, all the minors of $I(\lambda)_{,0}$ and $I(\lambda)_{,1}$ yield non-trivial polynomial equations in λ and therefore there are just finitely many values for λ for which any of these minors vanishes. In particular there is a $\gamma_1 \in \mathbb{C}$ such that both $I(\gamma_1)_{,0}$ and $I(\gamma_1)_{,1}$ are totally non-singular. Applying the same argument to $J(\lambda) := D_0 + \gamma_1 D_2 + \lambda D_2$ yields a $\gamma_2 \in \mathbb{C}$ such that $J(\gamma_2)_{,0}$, $J(\gamma_2)_{,1}$ and $J(\gamma_2)_{,2}$ are totally non-singular. Continuing to choose the γ_i, $i \in \{1, \dots, n\}$, inductively in this fashion then yields a totally non-singular matrix B with $A^* B = 0$. □

Lemma V.2. *Let $q \in \{1, \dots, n-1\}$ and let $A \in M(n, q, \mathbb{R})$ be totally non-singular. Then, there exists a totally non-singular matrix $B \in M(n, n-q, \mathbb{R})$ such that $A^t B = 0$.*

Proof. The arguments given in the proof of Lemma V.1 also apply to real numbers. □

For $k \in \{1, \dots, 2n-3\}$, define the inclusion in the k-th antidiagonal $\iota_k : \mathbb{C}^{\gamma(n,k)} \to H(n)$ by

$$(\iota_k(v))_{jl} := \frac{1}{\sqrt{2}} \begin{cases} v_j & \text{if } j + l = k, j < l \\ v_l^* & \text{if } j + l = k, l < j \\ 0 & \text{else} \end{cases}$$

where

$$\gamma(n,k) = \begin{cases} \lceil k/2 \rceil & \text{if } k \leq n-1 \\ \lceil n - 1 - k/2 \rceil & \text{if } k > n-1 \end{cases}$$

is the length of the upper half of the k-th antidiagonal. By expanding in the generalised Gell-Mann orthonormal basis of $H(n)$, it is easily seen that the inclusion of real vectors in the same antidiagonal preserves the standard inner product, i.e. for $k \in \{1, \dots, 2n-3\}$ we have

$$\operatorname{tr}\big(\iota_k(v) \iota_k(w)\big) = \langle v, w \rangle, \ \forall v, w \in \mathbb{R}^{\gamma(n,k)}. \tag{8}$$

Furthermore, the inclusion of an imaginary and a real vector in the same antidiagonal yields Hilbert-Schmidt orthogonal matrices, i.e. for $k \in \{1, \dots, 2n-3\}$ we have

$$\operatorname{tr}\big(\iota_k(v) \iota_k(iw)\big) = 0, \ \forall v, w \in \mathbb{R}^{\gamma(n,k)}, \tag{9}$$

and finally that inclusions of vectors in different antidiagonals also yield Hilbert-Schmidt orthogonal matrices, i.e. for $k, j \in \{1, \dots, 2n-3\}$ with $k \neq j$ we have

$$\operatorname{tr}\big(\iota_k(v) \iota_j(w)\big) = 0, \ \forall v \in \mathbb{C}^{\gamma(n,k)}, w \in \mathbb{C}^{\gamma(n,j)}. \tag{10}$$

The following theorem is the main result of the present paper.

Theorem V.3. *Let G_0 be a basis of C_r^n* [13]*. Furthermore, for $k \in \{2r-1, \dots, 2(n-r)-1\}$, let $A_k, A'_k \in M(\gamma(n,k), r, \mathbb{R})$ be totally non-singular and define the tuple*

$$G_k := \big(\iota_k(A_k[0]), \iota_k(iA'_k[0]), \iota_k(A_k[1]), \iota_k(iA'_k[1]), \dots, \iota_k(A_k[r-1]), \iota_k(iA'_k[r-1])\big).$$

Then $G := G_0 \cup G_{2r-1} \cup G_{2r} \cup \cdots \cup G_{2(n-r)-1}$ is r-complete and $|G| = 4r(n-r) + n - 2r$.

Proof. The idea of the proof is to use Lemma V.2 to determine a basis of the null space of M_G such that the construction of [19] can be applied. We do this in the first step of the proof. In the second step of the proof we use the construction of [19] to show that M_G indeed is r-complete.

Step 1. First, by Lemma V.2, there are totally non-singular $B_k, B'_k \in M(\gamma(n,k), \gamma(n,k)-r, \mathbb{R})$, $k \in \{2r+1, \dots, 2(n-r)-3\}$, such that

$$\begin{aligned} A_k^t B_k &= 0, \\ (A'_k)^t B'_k &= 0. \end{aligned} \tag{11}$$

Now let

$$G_k^\perp := \big(\iota_k(B_k[0]), \iota_k(iB'_k[0]), \dots, \iota_k(B_k[\gamma(n,k)-r-1]), \iota_k(iB'_k[\gamma(n,k)-r-1])\big), \quad k \in \{2r+1, \dots, 2(n-r)-3\}$$

and let $G_k^\perp = (0)$ for $k \in \{2r-1, 2r, 2(n-r)-2, 2(n-r)-1\}$. In the remainder of this first step we prove that $G_{2r-1}^\perp \cup \cdots \cup G_{2(n-r)-1}^\perp$ is a basis of $\mathrm{Ker}(M_G)$: For $k \in \{1, \dots, 2n-3\}$, let $Q_k := \{X \in H(n) : X(j) = 0 \ \forall j \neq k \ \wedge \ X_{ii} = 0 \text{ for } 2i = k\}$ be the subspace of Hermitian matrices with vanishing diagonal and non-vanishing entries only in the k-th antidiagonal. By Equation (10), $H(n)$ can be decomposed into the following mutually orthogonal subspaces:

$$H(n) = C_r^n \oplus Q_{2r-1} \oplus \cdots \oplus Q_{2(n-r)-1}. \tag{12}$$

Note that $\mathrm{Span}(G_k \cup G_k^\perp) \subseteq Q_k$ for all $k \in \{2r-1, \dots, 2(n-r)-1\}$. Hence, by the decomposition (12), to show that $G_{2r-1}^\perp \cup \cdots \cup G_{2(n-r)-1}^\perp$ is a basis of $\mathrm{Ker}(M_G)$ it suffices to prove that for $k \in \{2r-1, \dots, 2(n-r)-1\}$ the matrices $G_k^\perp \cup G_k$ span the subspace Q_k and that $\mathrm{Span}(G_k^\perp) \subseteq \mathrm{Ker}(M_G)$. First observe that indeed $\mathrm{Span}(G_k^\perp) \subseteq \mathrm{Ker}(M_G)$ for every $k \in \{2r+1, \dots, 2(n-r)-3\}$: Note that for every $k \in \{2r+1, \dots, 2(n-r)-3\}$,

$$\begin{aligned} \mathrm{tr}\big(\iota_k(A_k[l])\iota_k(B_k[j])\big) &= \langle A_k[l], B_k[j]\rangle = (A_k^t B_k)_{lj} = 0, \\ \mathrm{tr}\big(\iota_k(iA'_k[l])\iota_k(iB'_k[j])\big) &= \langle A'_k[l], B'_k[j]\rangle = ((A'_k)^t B'_k)_{lj} = 0, \\ \forall l \in \{0, \dots, r-1\},\ j &\in \{0, \dots, \gamma(n,k)-r-1\}, \end{aligned} \tag{13}$$

by equations (8) and (11). Furthermore,

$$\begin{aligned} \mathrm{tr}\big(\iota_k(iA'_k[l])\iota_k(B_k[j])\big) &= 0, \\ \mathrm{tr}\big(\iota_k(A_k[l])\iota_k(iB'_k[j])\big) &= 0, \\ \forall l \in \{0, \dots, r-1\},\ j &\in \{0, \dots, \gamma(n,k)-r-1\}, \end{aligned} \tag{14}$$

[13] C_r^n was defined in Equation (4).

by Equation (9). I.e. $\mathrm{Span}(G_k^\perp)$ is orthogonal to $\mathrm{Span}(G_k)$ and thus $\mathrm{Span}(G_k^\perp) \subseteq \mathrm{Ker}(M_G)$.

To conclude the first step, we prove that $G_k^\perp \cup G_k$ spans the subspace Q_k for every $k \in \{2r-1, \ldots, 2(n-r)-1\}$: Let $k \in \{2r-1, \ldots, 2(n-r)-1\}$. Since A_k is totally non-singular, the columns of A_k are linearly independent and the same argument applies to A_k'. Hence, by the equations (8) and (9), G_k is a tuple of linearly independent Hermitian matrices. The same argument applies to $G_k^\perp$, $k \in \{2r+1, \ldots, 2(n-r)-3\}$. But we have seen that $\mathrm{Span}(G_k)$ is orthogonal to $\mathrm{Span}(G_k^\perp)$ for $k \in \{2r+1, \ldots, 2(n-r)-3\}$. Furthermore, for $k \in \{2r-1, \ldots, 2(n-r)-1\}$, $|G_k^\perp| + |G_k| = 2(\gamma(n,k)-r) + 2r = 2\gamma(n,k) = \dim Q_k$ and thus $G_k^\perp \cup G_k$ indeed spans Q_k.

Finally, observe that

$$\begin{aligned} |G| &= \dim C_r^n + \sum_{i=2r-1}^{2(n-r)-1} |G_i| = \sum_{i=1}^{2r-2} 2\gamma(n,i) + n + \sum_{i=1}^{2(n-2r)+1} 2r \\ &= (2r)^2 - 2(2r) + n + 2r(2(n-2r)+1) \\ &= 4r(n-r) + n - 2r. \end{aligned}$$

Step 2. In the second step, we essentially reproduce the construction of [19] and some ideas of [26]. We show in the following that every nonzero matrix $X \in \mathrm{Ker}(M_G)$ has at least $r+1$ positive and $r+1$ negative eigenvalues and this concludes the proof by Proposition II.2.

Let $X \in \mathrm{Ker}(M_G)$ be arbitrary. By the interlaced eigenvalue Theorem (Theorem 4.3.15 of [28]) it suffices to prove that there is an $2(r+1) \times 2(r+1)$ principal submatrix of X with $r+1$ positive and $r+1$ negative eigenvalues. We conclude the proof by finding such a submatrix: There is a smallest number $k \in \{2r+1, \ldots, 2(n-r)-3\}$ such that X has non-vanishing entries in the k-th antidiagonal. First note that either the real or the imaginary part of the k-th antidiagonal does not vanish. Let us consider the case where the real part does not vanish, the other case can be shown analogously. The real part of the k-th antidiagonal of $\mathrm{Ker}(M_G)$ is spanned by the $\gamma(n,k)-r$ real matrices of $G_k^\perp$, i.e. each $X \in \mathrm{Ker}(M_G)$ is a linear combination of the $\gamma(n,k)-r$ real matrices of $G_k^\perp$. But then there have to be at least $2(r+1)$ non-vanishing entries in the k-th antidiagonal of X because otherwise there would be a vanishing $(\gamma(n,k)-r) \times (\gamma(n,k)-r)$ minor of B_k and this contradicts the fact that B_k is totally non-singular (For more details see Lemma 9 of [26].). I.e. there is a $2(r+1) \times 2(r+1)$ principal submatrix of X of the from:

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & \overline{x}_1 \\ 0 & 0 & 0 & \ldots & 0 & \overline{x}_2 & \overline{y}_1^1 \\ 0 & 0 & 0 & \ldots & \overline{x}_3 & \overline{y}_1^2 & \overline{y}_2^1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & x_3 & \ldots & 0 & \overline{y}_{2r-2}^2 & \overline{y}_{2r-1}^1 \\ 0 & x_2 & y_1^2 & \ldots & y_{2r-2}^2 & 0 & \overline{y}_{2r}^1 \\ x_1 & y_1^1 & y_2^1 & \ldots & y_{2r-1}^1 & y_{2r}^1 & 0 \end{pmatrix}, x_i \in \mathbb{C} \setminus \{0\},\ i \in \{1, \ldots, r+1\}, \tag{15}$$

where $y_i^j \in \mathbb{C},\ j \in \{1, \ldots, r\}, i \in \{1, \ldots, 2(r+1)-2j\}$, are arbitrary.

Finally, we show by induction that a matrix of this form has at least $r+1$ positive and $r+1$ negative eigenvalues: The claim clearly holds for $r = 0$. Now assume the claim

holds for $r \in \mathbb{N}_0$. Let Y be a $2(r+2) \times 2(r+2)$ matrix that is of the form illustrated in Equation (15). Then, one can obtain a principal $2(r+1) \times 2(r+1)$ submatrix Y' of Y that is of the same form by e.g. deleting the first and last row as well as the first and last column of Y. Thus, by the induction hypothesis and the interlaced eigenvalue Theorem (Theorem 4.3.15 of [28]), Y has at least $r+1$ positive and $r+1$ negative eigenvalues. A straightforward calculation shows that $\det(Y) \cdot \det(Y') < 0$. Since the determinant of a matrix is the product of its eigenvalues, the claim follows from $\det(Y) \cdot \det(Y') < 0$. □

In the following the $r = 1$ case is of particular interest because Theorem III.1 is obtained from this case by choosing the totally non-singular matrices appropriately.

Corollary V.4. *Let $G_0 := (e_0 e_0^*, \ldots, e_{n-1} e_{n-1}^*)$. Furthermore let $w_k, v_k \in \mathbb{R}^{\gamma(n,k)}$, $k \in \{1, \ldots, 2n-3\}$, be such that every entry of v_k and every entry of w_k is nonzero. Then $G := G_0 \cup \big(\iota_1(v_1), \iota_1(iw_1)\big) \cup \cdots \cup \big(\iota_{2n-3}(v_{2n-3}), \iota_{2n-3}(iw_{2n-3})\big)$ is 1-complete and $|G| = 5n-6$.*

Proof. First, note that G_0 is a basis of C_1^n. Furthermore as by assumption all entries of matrices $w_k, v_k \in \mathbb{R}^{\gamma(n,k)} \simeq M(\gamma(n,k), 1, \mathbb{R})$, $k \in \{1, \ldots, 2n-3\}$, are nonzero, we conclude that all their minors are nonzero[14]. Consequently the matrices $w_k, v_k \in M(\gamma(n,k), 1, \mathbb{R})$, $k \in \{1, \ldots, 2n-3\}$, are totally non-singular. Hence G_0 and $G_k := \big(\iota_1(v_1), \iota_1(iw_1)\big)$, $k \in \{1, \ldots, 2n-3\}$ fulfil the conditions of Theorem V.3 for $r = 1$ and thus $G = G_0 \cup G_1 \cup \ldots \cup G_{2n-3}$ is 1-complete. □

Example For $i \in \{1, \ldots, 2n-3\}$, we can choose $w_i = v_i = \sqrt{2}e$, where $e := (1, \ldots, 1) \in \mathbb{R}^{\gamma(n,i)}$ is the vector with a one in every component. Altogether this yields $2(2n-3)+n = 5n-6$ Hermitian operators for G. For $n = 4$ these are

$$\begin{pmatrix} 1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&i&0&0\\-i&0&0&0\\0&0&0&0\\0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\0&0&0&0\\1&0&0&0\\0&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&i&0\\0&0&0&0\\-i&0&0&0\\0&0&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&i\\0&0&i&0\\0&-i&0&0\\-i&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0\\0&0&0&1\\0&0&0&0\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0\\0&0&0&i\\0&0&0&0\\0&-i&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0\\0&0&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&0\\0&0&0&0\\0&0&0&i\\0&0&-i&0 \end{pmatrix}.$$

Finally, let us give a proof of Theorem III.3.

Proof. For $k \in \{2r-1, \ldots, 2(n-r)-1\}$, define $A_k, A'_k \in M(\gamma(n,k), r, \mathbb{R})$ by setting $(A_k)_{jl} = (A'_k)_{jl} = x_{l+1}^j$ for all $j \in \{0, \ldots, \gamma(n,k)-1\}, l \in \{0, \ldots, r-1\}$. Observe that both A_k and A'_k can be considered as the first r columns of a $\gamma(n,k) \times \gamma(n,k)$ Vandermonde matrix and since $x_j \neq x_l$ for all $j, l \in \{1, \ldots, r\}$ with $j \neq l$ and $x_l \neq 0$ for all $l \in \{1, \ldots, r\}$ they are thus totally non-singular. Applying Theorem V.3 to A_k, A'_k then concludes the proof. □

[14] The minors of a $m \times 1$ matrix are simply the entries of the matrix.

B. Proof of Theorem III.1

Let us now give a proof of Theorem III.1.

Proof. Define $Y_k, X_k \in H(n),\ k \in \{1,\dots,2n-3\}$, by

$$(X_k)_{jl} := \delta_{j+l,k} \cos\left(\frac{j-l}{2n}\pi\right),$$
$$(Y_k)_{jl} := i\delta_{j+l,k} \sin\left(\frac{j-l}{2n}\pi\right),$$
$$j,l \in \{0,\dots,n-1\}.$$

Next observe two things:

1. The matrices $\{X_1, Y_1, \dots, X_{2n-3}, Y_{2n-3}\} \subseteq H(n)$ are linearly independent by equations (9) and (10).

2. Since $0 < \frac{j-l}{2n}\pi < \frac{\pi}{2}$ for $j,l \in \{0,\dots,n-1\}$, $j > l$, we find $(X_k)_{jl} \neq 0$ and $(Y_k)_{jl} \neq 0$ for $j + l = k$, $j > l$.

Let $u_k, w_k \in \mathbb{R}^{\gamma(n,k)},\ k \in \{1,\dots,2n-3\}$, be such that $\iota_k(u_k) = X_k - \delta_{k/2,\lceil k/2\rceil} e_{\lceil k/2\rceil} e^*_{\lceil k/2\rceil}$, $\iota_k(iw_k) = Y_k$ and note that both u_k and w_k have no vanishing entry. Thus, by Corollary V.4, $\tilde{G} := (e_0e_0^*, \dots, e_{n-1}e_{n-1}^*) \cup (X_1, Y_1, \dots, X_{2n-3}, Y_{2n-3})$ is 1-complete.

Let $G := (e_0e_0^*, \dots, e_{n-1}e_{n-1}^*, v_1v_1^*, \overline{v}_1\overline{v}_1^*, \dots, v_{2n-3}v_{2n-3}^*, \overline{v}_{2n-3}\overline{v}_{2n-3}^*)$. To conclude the proof, we show that $\mathrm{Span}(G) = \mathrm{Span}(\tilde{G})$. First note that for $k \in \{1,\dots,2n-3\}$

$$v_kv_k^* = \sum_{j=1}^{2n-3} x_k^j (X_j + Y_j) + e_0e_0^* + x_k^{2n-2} e_{n-1}e_{n-1}^*,$$
$$\overline{v}_k\overline{v}_k^* = \sum_{j=1}^{2n-3} x_k^j (X_j - Y_j) + e_0e_0^* + x_k^{2n-2} e_{n-1}e_{n-1}^*$$

and thus $\mathrm{Span}(G) \subseteq \mathrm{Span}(\tilde{G})$. In order to show that $\mathrm{Span}(\tilde{G}) \subseteq \mathrm{Span}(G)$, consider the matrix

$$T := \begin{pmatrix} x_1 & x_1^2 & x_1^3 & \dots & x_1^{2n-3} \\ x_2 & x_2^2 & x_2^3 & \dots & x_2^{2n-3} \\ x_3 & x_3^2 & x_3^3 & \dots & x_3^{2n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ x_{2n-3} & x_{2n-3}^2 & x_{2n-3}^3 & \dots & x_{2n-3}^{2n-3}. \end{pmatrix}$$

The matrix T is a Vandermonde matrix and thus invertible if $x_i \neq x_j$ for $i \neq j$. Hence we

find [15]

$$X_k = \frac{1}{2}\sum_{j=1}^{2n-3}(T^{-1})_{kj}(v_j v_j^* + \overline{v}_j\overline{v}_j^* - 2e_0e_0^* - 2x_k^{2n-2}e_{n-1}e_{n-1}^*),$$
$$Y_k = \frac{1}{2}\sum_{j=1}^{2n-3}(T^{-1})_{kj}(v_j v_j^* - \overline{v}_j\overline{v}_j^*)$$

and this shows that $\mathrm{Span}(\tilde{G}) \subseteq \mathrm{Span}(G)$. □

Remark Note that there are many possible choices for the phases of the v_i. The only constraint is that $j\varphi \neq \frac{k\pi}{2}$ for all $j \in \{1,\ldots,n-1\},\ k \in \mathbb{Z}$.

C. Proof of Theorem IV.1 and Proposition IV.2

For $X_r \in \mathcal{S}_r^n$, $E \in H(n)$, $\epsilon \geq 0$ and a measurement M define the set

$$F_\epsilon(X_r, E, M) := \{Y \in \mathcal{S}^n : \|M(Y) - b\|_2 \leq \epsilon\}, \tag{16}$$

where $b = M(X_r + E)$.

Lemma V.5. *(Stability.) Let M be an r-complete measurement and let $\epsilon > 0$. Then, there exists a constant $C_M > 0$ independent of ϵ such that for all $X_r \in \mathcal{S}_r^n$, and $E \in H(n)$ with $\|M(E)\|_2 \leq \epsilon$ we have*

$$Y \in F_\epsilon(X_r, E, M) \Rightarrow \|Y - X_r\|_2 \leq C_M\epsilon.$$

Proof. Denote by $\pi : H(n) \to \mathrm{Range}(M^*)$ the orthogonal projection on the subspace $\mathrm{Range}(M^*) \subseteq H(n)$ and by $\pi^\perp : H(n) \to \mathrm{Ker}(M)$ the orthogonal projection on the subspace $\mathrm{Ker}(M) \subseteq H(n)$. Furthermore, let $Y' := \pi^\perp(X_r) + \pi(Y)$ and let σ_{min} be the smallest singular value of M [16]. Then, we find

$$\begin{aligned}\|X_r - Y'\| = \|\pi(X_r - Y)\|_2 &\leq \frac{1}{\sigma_{min}}\|M(Y - X_r)\|_2 \\ &\leq \frac{1}{\sigma_{min}}(\|M(X_r) - b\|_2 + \|M(Y) - b\|_2) \leq \frac{1}{\sigma_{min}}(\|M(E)\|_2 + \epsilon) \\ &\leq \frac{2}{\sigma_{min}}\epsilon. \end{aligned} \tag{17}$$

From the spectral variation bound for Hermitian matrices (Theorem III.2.8 of [29]) we conclude that

$$\begin{aligned}\|\mathrm{Eig}(X_r) - \mathrm{Eig}(Y')\|_2 &= \sqrt{\sum_{i=1}^{r}\left(\lambda_i(X_r) - \lambda_i(Y')\right)^2 + \sum_{i=r+1}^{n}\lambda_i(Y')^2} \\ &\leq \frac{2}{\sigma_{min}}\epsilon.\end{aligned}$$

[15] Different from the rest of the present paper, the indices we use to label T begin with 1, not with G.
[16] We assume M to have full rank.

But this implies that $|\lambda_i(Y')| \leq \frac{2}{\sigma_{min}}\epsilon$ for $i \in \{r+1, \ldots, n\}$.

Next, note that

$$\kappa := - \max_{Z \in \mathrm{Ker}(M), \|Z\|_2 = 1} \lambda_{n-r}(Z)$$

exists by compactness of $\{Z \in \mathrm{Ker}(M) : \|Z\|_2 = 1\}$ and continuity of λ_{n-r}. Furthermore, by Proposition II.2, every nonzero $Z \in \mathrm{Ker}(M)$ has at least $r+1$ negative eigenvalues and hence we conclude that $\kappa > 0$.

There exists $Z \in \mathrm{Ker}(M)$ with $\|Z\|_2 = 1$ and $\alpha \geq 0$ such that $Y = Y' + \alpha Z$ [17]. Since $Y \geq 0$ we conclude from Weyl's inequality (Theorem III.2.1 of [29]) that

$$0 \leq \lambda_n(Y' + \alpha Z) \leq \lambda_{r+1}(Y') + \alpha \lambda_{n-r}(Z) \leq \frac{2}{\sigma_{min}}\epsilon - \alpha\kappa.$$

and hence we find

$$\alpha \leq \frac{2}{\kappa \sigma_{min}}\epsilon. \tag{18}$$

Finally, combining equations (17) and (18), we conclude that

$$\begin{aligned} \|Y - X_r\|_2 = \|Y' + \alpha Z - X_r\|_2 &\leq \|Y' - X_r\|_2 + \|\alpha Z\|_2 \\ &\leq \left(\frac{2}{\sigma_{min}} + \frac{2}{\kappa \sigma_{min}} \right) \epsilon. \end{aligned}$$

Choosing $C_M = \frac{2}{\sigma_{min}}(1 + \frac{1}{\kappa})$ then proves the claim. □

Remark Since κ just depends on $\mathrm{Ker}(M)$, it is independent of the choice of basis for $\mathrm{Range}(M^*)$. Thus, since it is always possible to choose an orthonormal basis of $\mathrm{Range}(M^*)$, the constant C_M is mainly determined by κ.

The proof of Theorem IV.1 is an immediate consequence of this lemma.

Remark Let M be a measurement that is not r-complete. Then there exist $Z_r \in \mathcal{S}_r^n$ and $Z \in \mathcal{S}^n$ with $Z_r \neq Z$ such that $M(Z_r - Z) = 0$ and we find $Z \in F_\epsilon(Z_r, E, M)$ for all $\epsilon > 0$ and $E \in H(n)$ with $\|M(E)\|_2 \leq \epsilon$. Thus, if $\mathbb{1} \in \mathrm{Range}(M^*)$, the r-complete property is necessary to enable the recovery of every $X_r \in \mathcal{S}_r^n$ via the optimization problem (5).

Finally let us give the proof of Proposition IV.2.

Proof. From Theorem IV.1 we obtain the bound $\|Y - xx^*\|_2 \leq C_M\epsilon$ and the proof of Lemma IV yields the bound $\sqrt{\sum_{i=2}^n \lambda_i(Y)^2} \leq C_M\epsilon$. From this we find

$$\|xx^* - \hat{x}\hat{x}^*\|_2 \leq \|Y - xx^*\|_2 + \|Y - \hat{x}\hat{x}^*\|_2 \leq 2C_M\epsilon.$$

[17] Note that $\alpha Z = \pi^\perp(Y) - \pi^\perp(X_r) \in \mathrm{Ker}(M)$.

Finally let $\varphi \in [0, 2\pi)$ be such that $\langle x, e^{i\varphi}\hat{x}\rangle$ is positive. Then,

$$\begin{aligned}
\|x - e^{i\varphi}\hat{x}\|_2^2\|x\|_2^2 &= \left(\|x\|_2^2 + \|\hat{x}\|_2^2 - 2\mathrm{Re}\left(\langle x, e^{i\varphi}\hat{x}\rangle\right)\right)\|x\|_2^2 \\
&= \left(\|x\|_2^2 + \|\hat{x}\|_2^2 - 2|\langle x, \hat{x}\rangle|\right)\|x\|_2^2 \\
&\leq \left(\|x\|_2^2 + \|\hat{x}\|_2^2 - 2|\langle x, \hat{x}\rangle|\right)\left(\|x\|_2^2 + \|\hat{x}\|_2^2 + 2|\langle x, \hat{x}\rangle|\right) \\
&= \left(\|x\|_2^2 + \|\hat{x}\|_2^2\right)^2 - 4|\langle x, \hat{x}\rangle|^2 \\
&= \|x\|_2^4 + \|\hat{x}\|_2^4 - 2|\langle x, \hat{x}\rangle|^2 + 2\|x\|_2^2\|\hat{x}\|_2^2 - 2|\langle x, \hat{x}\rangle|^2 \\
&\leq 2\left(\|x\|_2^4 + \|\hat{x}\|_2^4 - 2|\langle x, \hat{x}\rangle|^2\right) \\
&= 2\|xx^* - \hat{x}\hat{x}^*\|_2^2 \\
&\leq 2(2C_M\epsilon)^2.
\end{aligned}$$

□

---

[1] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Applied and Computational Harmonic Analysis*, 20(3):345–356, 2006.

[2] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. *Applied and Computational Harmonic Analysis*, 2014.

[3] Michael Kech and Michael M. Wolf. Quantum tomography of semi-algebraic sets with constrained measurements. *arXiv:1507.00903*, 2015.

[4] Damien Mondragon and Vladislav Voroninski. Determination of all pure quantum states from a minimal number of observables. *arXiv preprint arXiv:1306.1214*, 2013.

[5] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. How many orthonormal bases are needed to distinguish all pure quantum states? *arXiv preprint arXiv:1504.01590*, 2015.

[6] Teiko Heinosaari, Luca Mazzarella, and Michael M Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318(2):355–374, 2013.

[7] Matthew Fickus, Dustin G Mixon, Aaron A Nelson, and Yang Wang. Phase retrieval from very few measurements. *Linear Algebra and its Applications*, 449:475–499, 2014.

[8] Radu Balan, Bernhard G Bodmann, Peter G Casazza, and Dan Edidin. Painless reconstruction from magnitudes of frame coefficients. *Journal of Fourier Analysis and Applications*, 15(4):488–501, 2009.

[9] Boris Alexeev, Afonso S Bandeira, Matthew Fickus, and Dustin G Mixon. Phase retrieval with polarization. *SIAM Journal on Imaging Sciences*, 7(1):35–66, 2014.

[10] Afonso S Bandeira, Yutong Chen, and Dustin G Mixon. Phase retrieval from power spectra of masked signals. *Information and Inference*, page iau002, 2014.

[11] Emmanuel J Candes, Yonina C Eldar, Thomas Strohmer, and Vladislav Voroninski. Phase retrieval via matrix completion. *SIAM Review*, 57(2):225–251, 2015.

[12] Emmanuel J Candes, Thomas Strohmer, and Vladislav Voroninski. Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming. *Communications on Pure and Applied Mathematics*, 66(8):1241–1274, 2013.

[13] Emmanuel J Candes and Xiaodong Li. Solving quadratic equations via phaselift when there are about as many equations as unknowns. *Foundations of Computational Mathematics*, 14(5):1017–1026, 2014.

[14] Emmanuel J Candes, Xiaodong Li, and Mahdi Soltanolkotabi. Phase retrieval via wirtinger flow: Theory and algorithms. *IEEE Transactions on Information Theory*, 61(4):1985–2007, 2015.

[15] David Gross, Felix Krahmer, and Richard Kueng. A partial derandomization of phaselift using spherical designs. *Journal of Fourier Analysis and Applications*, 21(2):229–266, 2015.

[16] Richard Kueng, David Gross, and Felix Krahmer. Spherical designs as a tool for derandomization: The case of phaselift. In *11th international conference on Sampling Theory and Applications (SampTA 2015), Washington, USA*, 2015.

[17] Bernhard G Bodmann and Nathaniel Hammen. Stable phase retrieval with low-redundancy frames. *Advances in computational mathematics*, 41(2):317–331, 2015.

[18] Bernhard G Bodmann and Nathaniel Hammen. Algorithms and error bounds for noisy phase retrieval with low-redundancy frames. *Applied and Computational Harmonic Analysis*, 2016.

[19] Jianxin Chen, Hillary Dawkins, Zhengfeng Ji, Nathaniel Johnston, David Kribs, Frederic Shultz, and Bei Zeng. Uniqueness of quantum states compatible with given measurement results. *Physical Review A*, 88(1):012109, 2013.

[20] Emmanuel J Candès and Benjamin Recht. Exact matrix completion via convex optimization. *Foundations of Computational mathematics*, 9(6):717–772, 2009.

[21] Emmanuel J Candes and Yaniv Plan. Matrix completion with noise. *Proceedings of the IEEE*, 98(6):925–936, 2010.

[22] Emmanuel J Candès and Terence Tao. The power of convex relaxation: Near-optimal matrix completion. *Information Theory, IEEE Transactions on*, 56(5):2053–2080, 2010.

[23] Benjamin Recht, Maryam Fazel, and Pablo A Parrilo. Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization. *SIAM review*, 52(3):471–501, 2010.

[24] David Gross, Yi-Kai Liu, Steven T Flammia, Stephen Becker, and Jens Eisert. Quantum state tomography via compressed sensing. *Physical review letters*, 105(15):150401, 2010.

[25] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. Tasks and premises in quantum state determination. *Journal of Physics A: Mathematical and Theoretical*, 47(7):075302, 2014.

[26] Toby Cubitt, Ashley Montanaro, and Andreas Winter. On the dimension of subspaces with bounded schmidt rank. *Journal of Mathematical Physics*, 49(2):022107, 2008.

[27] Michael Kech, Péter Vrana, and Michael Wolf. The role of topology in quantum tomography. *Journal of Physics A: Mathematical and Theoretical*, 48(26):265303, 2015.

[28] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

[29] Rajendra Bhatia. *Matrix analysis*, volume 169. Springer Science & Business Media, 2013.

Optimal Injectivity Conditions for Bilinear Inverse Problems with Applications to Identifiability of Deconvolution Problems

M. Kech and F. Krahmer August 24, 2016

In bilinear inverse problems the aim is to reconstruct two vectors $u \in \mathbb{C}^{n_1} \setminus \{0\},\ v \in \mathbb{C}^{n_2} \setminus \{0\}$ from the measurement outcome $\tilde{B}(u,v)$, where $\tilde{B} : \mathbb{C}^{n_1} \times \mathbb{C}^{n_2} \to \mathbb{C}^m$ is a bilinear map. At best, this is possible up to the equivalence relation $(u,v) \sim (\lambda u, 1/\lambda v),\ \lambda \in \mathbb{C} \setminus \{0\}$.

Definition 1. (Strong identifiability modulo scaling [1].) A subset $V \subseteq \mathbb{C}^{n_1} \setminus \{0\} \times \mathbb{C}^{n_2} \setminus \{0\}$ is strongly identifiable modulo scaling with respect to a bilinear map $\tilde{B} : \mathbb{C}^{n_1} \times \mathbb{C}^{n_2} \to \mathbb{C}^m$ iff the following condition holds: If there exist $(u,v),(u',v') \in V$ such that $\tilde{B}(u,v) = \tilde{B}(u',v')$, then $(u,v) \sim (u',v')$.

1 Tight Bounds for the Injectivity Problem

Let $\mathbb{C}^n_s := \{x \in \mathbb{C}^n :\ x \text{ is } s\text{-sparse}\}$ and let

$$M^1_{s_1,s_2}(n_1,n_2) := \{uv^t :\ u \in \mathbb{C}^{n_1}_{s_1},\ v \in \mathbb{C}^{n_2}_{s_2}\}.$$

As they allow for a more convenient presentation, the results in this section are given in terms of linear maps $B : \mathbb{C}^{n_1 \times n_2} \to \mathbb{C}^m$ rather than bilinear maps[1] $\tilde{B} : \mathbb{C}^{n_1} \times \mathbb{C}^{n_2} \to \mathbb{C}^m$.

Definition 2 (Stably (s_1,s_2)-injective)**.** A linear map $B : \mathbb{C}^{n_1 \times n_2} \to \mathbb{C}^m$ is called stably (s_1,s_2)-injective iff there exists a constant $C > 0$ such that $\|B(X)\| \geq C\|X\|_{HS}$ holds for all $X \in \{\lambda(X-Y) |\ X,Y \in M^1_{s_1,s_2}(n_1,n_2),\ \lambda > 0\}$.

The first result gives a general lower bound on the number of measurement outcomes of a stably (s_1,s_2)-injective linear map.

Theorem 1 (Lower bound)**.** *If the linear map $B : \mathbb{C}^{n_1 \times n_2} \to \mathbb{C}^m$ is stably (s_1,s_2)-injective, then*

$$m \geq \begin{cases} 2(n_1+n_2)-4 & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1+s_2)-2 & \text{else.} \end{cases}$$

The following theorem shows that the lower bound given by Theorem 1 is indeed tight.

[1] Recall that there is a one-to-one correspondence between bilinear maps $\tilde{B} : \mathbb{C}^{n_1} \times \mathbb{C}^{n_2} \to \mathbb{C}^m$ and linear maps $B : \mathbb{C}^{n_1 \times n_2} \to \mathbb{C}^m$.

Theorem 2 (Upper bound). *Almost all*[2] *linear maps* $B : \mathbb{C}^{n_1 \times n_2} \to \mathbb{C}^m$ *are stably* (s_1, s_2)*-injective if*

$$m \geq \begin{cases} 2(n_1 + n_2) - 4 & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1 + s_2) - 2 & \text{else.} \end{cases}$$

2 Blind Deconvolution

The circular convolution of vectors $v, w \in \mathbb{C}^m$ is denoted by $v \circledast w \in \mathbb{C}^m$, i.e., for all $i \in \{0, \dots, m-1\}$ one has $(v \circledast w)_i := \sum_{j=0}^{m-1} v_j w_{(i-j) \bmod m}$. The mapping

$$C : \mathbb{C}^m \times \mathbb{C}^m \to \mathbb{C}^m, \ (v, w) \mapsto v \circledast w$$

clearly is bilinear.

Denote by

$$F(m, k) := \{X \in \mathbb{C}^{m \times k} | \operatorname{rank} X = k\}$$

the set of all tuples of k linearly independent vectors in $\mathbb{C}^m$. In the following theorem the term "almost all" refers to the Lebesgue measure on $\mathbb{C}^{m \times k}$.

Theorem 3 (Deconvolution with sparsity constraint). *For* $E \in F(m, k)$*, set* $ran(E)_s := \{x \in ran\, E : x \text{ is } s\text{-sparse when expanded in } E.\}$*. Let* $s_1, s_2 \in \mathbb{N}_+$ *be such that* $2(s_1 + s_2) - 2 \leq m$ *and let* $k, l \in \mathbb{N}$ *be such that* $s_1 < k \leq m$*,* $s_2 < l \leq m$*. Then, for almost all pairs* $(E, D) \in F(m, k) \times F(m, l)$ *the set* $ran(E)_{s_1} \times ran(D)_{s_2}$ *is strongly identifiable modulo scaling with respect to the circular convolution map* $C : \mathbb{C}^m \times \mathbb{C}^m \to \mathbb{C}^m, \ (v, w) \mapsto v \circledast w$*.*

For $k \leq m$, consider the Grassmannian

$$G(m, k) := \{P \in \mathbb{C}^{m \times m} | \ P \text{ is a rank } k \text{ orthogonal projection.}\}.$$

Let d be the metric on $G(m, k)$ defined by setting $d(P, P') := \|P - P'\|_{HS}$ for all $P, P' \in G(m, k)$. In the following theorem, the term "almost all" refers to the Haar measure on the compact metric space $G(m, k) \times G(m, l)$.

Theorem 4 (Deconvolution with subspace constraint). *Let* $k, l \in \mathbb{N}_+$ *be such that* $2(k+l) - 4 \leq m$*. Then, for almost all pairs of projections* $(P, P') \in G(m, k) \times G(m, l)$ *the set* $ran\, P \times ran\, P'$ *is strongly identifiable modulo scaling with respect to the circular convolution map* $C : \mathbb{C}^m \times \mathbb{C}^m \to \mathbb{C}^m, \ (v, w) \mapsto v \circledast w$*.*

It follows form Theorem 1 that the bounds given in the theorems 3 and 4 are indeed optimal.

[2] By vectorizing the input matrices, the set of linear maps $B : \mathbb{C}^{n_1 \times n_2} \to \mathbb{C}^m$ can be identified with $\mathbb{C}^{n_1 n_2 \times m}$. The term "almost all" refers to the Lebesgue measure on $\mathbb{C}^{n_1 n_2 \times m}$.

3 Legal statement

I am the principal author of this article and I was significantly involved in all parts of this article.

References

[1] Yanjun Li, Kiryung Lee, and Yoram Bresler. Identifiability in blind deconvolution under minimal assumptions. preprint, arXiv:1507.01308, 2015.

Optimal Injectivity Conditions for Bilinear Inverse Problems with Applications to Identifiability of Deconvolution Problems

Michael Kech[1,*] and Felix Krahmer[1,†]

[1]*Department of Mathematics, Technische Universität München, 85748 Garching, Germany*

(Dated: March 23, 2016)

We study identifiability for bilinear inverse problems under sparsity and subspace constraints. We show that, up to a global scaling ambiguity, almost all such maps are injective on the set of pairs of sparse vectors if the number of measurements m exceeds $2(s_1+s_2)-2$, where s_1 and s_2 denote the sparsity of the two input vectors, and injective on the set of pairs of vectors lying in known subspaces of dimensions n_1 and n_2 if $m \geq 2(n_1+n_2)-4$. We also prove that both these bounds are tight in the sense that one cannot have injectivity for a smaller number of measurements. Our proof technique draws from algebraic geometry. As an application we derive optimal identifiability conditions for the deconvolution problem, thus improving on recent work of Li et al. [1].

Keywords: bilinear inverse problems, deconvolution, uniqueness

Contents

*Electronic address: kech@ma.tum.de
†Electronic address: felix.krahmer@tum.de

I. INTRODUCTION

While inverse problems have been subject of study for many years, a new viewpoint has been taken in the last years, starting with the fundamental works on compressed sensing [2, 3]. Namely, rather than assuming that the inverse problem is completely determined by the application and potentially maximally ill-posed, the paradigm was to use the remaining degrees of freedom in the problem design as much as possible to ensure a unique solution.

A common observation in many scenarios is that most measurement setups behave near optimally. There are two ways to make this precise and works following both approaches: On the one hand, one can choose the measurement parameters at random and study conditions entailing that recovery is possibly with high probability. On the other hand one can take an information theoretic approach, aiming to establish identifability (that is, solution uniqueness or injectivity) for all measurement parameters except for a set of measure zero. In contrast to the first approach, the goal is not to devise working solutions, but rather to establish fundamental limits for the number of measurements, which can then be used as a measure to judge the quality of a concrete measurement setup. As a consequence, the number of measurements needed in the second approach is smaller, but the resulting statement is weaker in the sense that much weaker claims are made about the stability with respect to noise and none about algorithms to find the unique solution.

These approaches have been extensively applied to linear inverse problems, that is, one considers linear measurements of a signal known to satisfy some additional model assumptions. In this context, the randomized approach is addressed in many works in the areas of compressed sensing – here the signal is assumed to be sparse –, low rank matrix recovery, and beyond (see [4] for a textbook with many references). The article [5] provides a comprehensive treatment to randomized linear inverse problems on a very general level via convex optimization. The linear setup has also been studied from the identifiability viewpoint. Under sparsity assumptions, this problem relates to the study of the spark of the measurement matrix, that is, (one more than) the largest number of linearly independent columns (cf. [6]). For low rank matrix recovery, identifiability conditions have been established in [7]. Again for low rank matrix recovery, identifiability conditions for random signal models have recently been studied in [8].

More recently, similar considerations have also been applied to the phase retrieval problem, where one still considers linear measurements, but only the (square of) their absolute values is observed. Recovery guarantees for randomized setups have first been proven in [9] and extended in many follow-up works. At the core of many of these works is a lifting idea, namely that phaseless measurements can be expressed as linear measurements on the outer product of the signal with itself. For the study of injectivity conditions, an algebraic geometry viewpoint has proven useful. It turned out to be crucial whether one deals with real or complex measurements. Optimal injectivity bounds (up to a global phase factor) for the real case were proven in [10], while the complex case has proven significantly more difficult and bounds have successively improved over the last few years [10–12].

For bilinear inverse problems, i.e., measurements that depend in a bilinear way on two input signals, such considerations are only in their beginnings. Here one can only hope for injectivity up to a global multiplicative constant. Again, via a lifting approach, such

problems can be identified with low rank matrix recovery problems. So if no structural constraints are imposed, recovery guarantees directly carry over. The setup with additional sparsity assumptions, again under random measurements, is somewhat more involved and has been studied in [13]. Deterministic conditions for injectivity are derived in [14], where the authors also consider scenarios where one only finds uniqueness up to more general multiplication groups.

Without additional assumptions, there is still a gap between both the randomized and the algebraic setup and measurement systems arising in applications. Namely, applications impose additional constraints on the structure of the measurements, which correspond to a measure zero set in the space of unrestricted measurements, so the aforementioned results typically do not have implications about whether any of the solutions satisfy these constraints. This motivated the study of structured random measurements in all the scenarios mentioned (see [15] for a survey on such approaches, not yet including bilinear problems). In compressed sensing, for example, randomly subsampled Fourier measurements have been considered [16], as motivated by applications in magnetic resonance imaging [17], as well as subsampled convolutions with a random vector [18], as motivated by applications in remote sensing and coded aperture imaging [19]. For low-rank matrix recovery, a measurement model arising in collaborative filtering application consists of randomly selected of matrix entries, which yields the so-called matrix completion problem [20]. For the phase retrieval problem, concatenations of Fourier measurements and random diagonal matrices have been studied, which are motivated by the idea of introducing a mask in a diffraction imaging setup [21–23].

Lastly, for bilinear inverse problems, two important classes of models that have been studied are calibration problems as well as blind deconvolution and demixing problems. From a randomization viewpoint, calibration problems have been studied in [24], blind deconvolution problems are studied in [25], and blind demixing problems are studied in [26]. All these papers are based again on lifting ideas. Identifiability conditions for calibration problems are derived in [14].

Identifiability for the blind deconvolution problem under sparsity or subspace constraints has first been studied in [27, 28], in particular providing negative results for signals sparse in the standard basis. Subsequently, this case has been identified as exceptional by providing identifiability results that hold for all sparsity bases except for a set of measure zero [29]. These results have then been improved to a near-optimal number of measurements [1]. The authors distinguish between weak and strong identifiability. The former notion relates to the number of measurements needed to ensure that for a given fixed signal and a generic set of sparsity bases, there is no other signal resulting in the same measurements; the latter requires that property uniformly for all potential signal. In the case of weak identifiability, the set of measurements, where the property fails is allowed to differ for each signal, so there will not necessarily be a set of bases for which one has injectivity, i.e., uniqueness for all signals at the same time.

Conditions for strong identifibiability in the blind deconvolution problem are also the main application of our results. The same techniques also yield conditions for weak identifiability (see Appendix B). In contrast to the result in [1], the our identifiability results for both cases are tight, that is, our theory implies matching upper and lower bounds for the

number of measurements needed. Also, our proof techniques are very different to those in [1]; our work is mainly based on techniques from algebraic geometry.

Outline. In Section II we fix notation and review the notions of weak and strong identifiability for bilinear inverse problems.

Then, in Section III, we give the main results of the present paper. We aim at discriminating any two pairs of vectors $(v,w),(v',w') \in \mathbb{C}^{n_1}\times\mathbb{C}^{n_2}$ up to the trivial scaling ambiguity from the outcomes $B(v,w)$, $B(v',w')$ of a bilinear measurement map $B : \mathbb{C}^{n_1}\times\mathbb{C}^{n_2} \to \mathbb{C}^m$ under the premise that v, v' are s_1-sparse and w, w' are s_2-sparse. We show that a bilinear map performing this task exists if and only if $m \geq 2(n_1+n_2)-4$ in case $s_1 = n_1$, $s_2 = n_2$ and $m \geq 2(s_1+s_2)-2$ otherwise.

In the second part of this section we apply our results to derive strong identfiability conditions for the deconvolution problem, which aims at identifying a signal $v \in \mathbb{C}^m$ and a filter $w \in \mathbb{C}^m$ up to the trivial scaling ambiguity from their circular convolution $v \circledast w$, and compare our results to previous work. Dimension counting already implies that blind deconvolution is infeasible in general, however identifiability may be possible when assuming $v \in V$ and $w \in W$ for some lower dimensional subspaces $V, W \subseteq \mathbb{C}^m$. Indeed we show that for generic subspaces $V, W \in \mathbb{C}^m$ it is possible to discriminate any two pairs of vectors $(v,w),(v',w') \in V \times W$ up to the trivial scaling ambiguity from their circular convolutions $v \circledast w$ and $v' \circledast w'$ if $2(\dim V + \dim W) - 4 \leq m$. The bound $m \geq 2(\dim V + \dim W) - 4$ is precisely the lower bound established in the first part of this section making this result optimal.

Furthermore we consider the scenario in which $v \in \mathbb{C}^{n_1}$ is assumed to be s_1-sparse in some basis $E \subseteq \mathbb{C}^{n_1}$ and $w \in \mathbb{C}^{n_2}$ is assumed to be s_2-sparse in some basis $D \subseteq \mathbb{C}^{n_2}$. Similar to the previous result we show that for generic bases E, D any two pairs of vectors $(v,w),(v',w') \in \mathbb{C}^{n_1}\times\mathbb{C}^{n_2}$ consistent with the sparsity constraints can be discriminated from their circular convolution up to the trivial scaling ambiguity if $2(s_1+s_2)-2 \leq m$. Again, since the bound $m \geq 2(s_1+s_2)-2$ is precisely the lower bound established in the first part of this section, this result is optimal.

The proofs of our main results are given in Section IV, some measure theoretic technicalities are deferred to Appendix A.

Our techniques also apply to the weak identifiability problem, i.e., the corresponding problem for (u,v) fixed. For this problem, in Appendix B, we also slightly improve the conditions derived in [1] in the case of sparsity constraints and show optimality.

II. PRELIMINARIES

Let us first fix some notation. We denote the Euclidean norm by $\|\cdot\|_2$. By $M(n_1,n_2)$ we denote the set of complex $n_1 \times n_2$ matrices. In the following we always assume $n_1, n_2 \geq 2$. The transpose (conjugate transpose) of a matrix $X \in M(n_1,n_2)$ is denoted by X^t (X^*). We equip $M(n_1,n_2)$ with the Hilbert-Schmidt inner product defined by setting $\langle X, Y\rangle = \operatorname{tr}(X^*Y)$ for all $X, Y \in M(n_1,n_2)$ and by $\|\cdot\|_F$ we denote the Hilbert-Schmidt/Frobenius norm. For $i \in \{1,\dots,n_1\}, j \in \{1,\dots,n_2\}$ we denote by X_i the i-th row and by X_{ij} the entry in the i-th row and j-th column of a matrix $X \in M(n_1,n_2)$. By $\mathbb{1}_n$ we denote the identity on $\mathbb{C}^n$. We denote by $M^r(n_1,n_2) \subseteq M(n_1,n_2)$ the set of complex matrices of rank

at most r. For $0 < s \leq n$ let $\mathbb{C}^n_s := \{x \in \mathbb{C}^n : x \text{ is } s\text{-sparse.}\}$. Furthermore let

$$M^1_{s_1,s_2}(n_1,n_2) := \{uv^t : u \in \mathbb{C}^{n_1}_{s_1}, v \in \mathbb{C}^{n_2}_{s_2}\}.$$

For two subsets $V, W \subseteq M(n_1,n_2)$ we define the set $V - W := \{X - Y : X \in V, Y \in W\}$ and we write $\Delta(V)$ as shorthand for $V - V$. By $\mathcal{L}(m)$ we denote the set of linear maps $M : M(n_1,n_2) \to \mathbb{C}^m$ and by $\mathcal{B}(m)$ we denote the set of bilinear maps $B : \mathbb{C}^{n_1} \times \mathbb{C}^{n_2} \to \mathbb{C}^m$. Finally, the kernel and the range of a linear map L are denoted by $\ker L$ and $\operatorname{ran} L$, respectively.

Using the Hilbert-Schmidt inner product we can identify $\mathcal{L}(m)$ with $(M(n_2,n_1))^m$. Indeed, for every linear map $M \in \mathcal{L}(m)$ there exists $(Y_1,\ldots,Y_m) \in (M(n_2,n_1))^m$ such that for all $X \in M(n_1,n_2)$ we have $M(X) = (\operatorname{tr}(Y_1X),\ldots,\operatorname{tr}(Y_mX))$ and conversely every $Y := (Y_1,\ldots,Y_m) \in (M(n_2,n_1))^m$ induces a linear map $M_Y \in \mathcal{L}(m)$ by setting

$$M_Y(X) := (\operatorname{tr}(Y_1X),\ldots,\operatorname{tr}(Y_mX)) \tag{1}$$

for all $X \in M(n_1,n_2)$.

In bilinear inverse problems the objective is to reconstruct two vectors $u \in \mathbb{C}^{n_1} \setminus \{0\}$, $v \in \mathbb{C}^{n_2} \setminus \{0\}$ form a measurement outcome $z = B(u,v) \in \mathbb{C}^m$ where $B \in \mathcal{B}(m)$ is a bilinear map. In the best case this can be done modulo the trivial ambiguity

$$B(u,v) = B(\lambda u, 1/\lambda v),\ \forall \lambda \in \mathbb{C} \setminus \{0\}.$$

This ambiguity naturally induces an equivalence relation on $\mathbb{C}^{n_1} \setminus \{0\} \times \mathbb{C}^{n_2} \setminus \{0\}$ and we denote the equivalence class of $(u,v) \in \mathbb{C}^{n_1} \setminus \{0\} \times \mathbb{C}^{n_2} \setminus \{0\}$ by $[(u,v)]$, i.e., $[(u,v)] = [(u',v')]$ for some $u' \in \mathbb{C}^{n_1} \setminus \{0\}$, $v' \in \mathbb{C}^{n_2} \setminus \{0\}$ if there exists $\lambda \in \mathbb{C} \setminus \{0\}$ such that $(u,v) = (\lambda u', 1/\lambda v')$.

This motivates the following notion of identifiability which is basically the same as part 2 of Definition 2.1 in [1].

Definition II.1. *(Strong identifiability modulo scaling.) A subset $V \subseteq \mathbb{C}^{n_1} \setminus \{0\} \times \mathbb{C}^{n_2} \setminus \{0\}$ is identifiable modulo scaling with respect to a map $B \in \mathcal{B}(m)$, if $B(u,v) = B(u',v')$ for some $(u,v),(u',v') \in V$ implies $[(u,v)] = [(u',v')]$.*

This strong notion of identifiability requires that every measurement corresponds to a unique signal. The following weaker notion, basically the same as part 1 of Definition 2.1 in [1], requires this only for the measurement arising from a given fixed signal.

Definition II.2. *(Weak identifiability modulo scaling.) The restriction of a map $B \in \mathcal{B}(m)$ to a subset $V \subseteq \mathbb{C}^{n_1} \setminus \{0\} \times \mathbb{C}^{n_2} \setminus \{0\}$ is weakly identifiable modulo scaling at (u_0,v_0) if $B(u,v) = B(u_0,v_0)$ for some $(u,v) \in V$ implies $[(u,v)] = [(u_0,v_0)]$.*

III. MAIN RESULTS

A. Tight Bounds for the Injectivity Problem

In the following we first obtain a general lower bound on the number $m \in \mathbb{N}$ for which there exists an (s_1,s_2)-injective bilinear map $B \in \mathcal{B}(m)$. Then, in a next step, we show that this lower bound is indeed tight.

It is well-known that there is a one-to-one correspondence between the sets $\mathcal{B}(m)$ and $\mathcal{L}(m)$. Indeed, every bilinear map $B : \mathbb{C}^{n_1} \times \mathbb{C}^{n_2} \to \mathbb{C}^m$ induces a unique linear map $M : M(n_1, n_2) \to \mathbb{C}^m$ such that for all $x \in \mathbb{C}^{n_1}, y \in \mathbb{C}^{n_2}$ we have $M(xy^t) = B(x, y)$. Conversely each linear map $M : M(n_1, n_2) \to \mathbb{C}^m$ induces a bilinear map $B : \mathbb{C}^{n_1} \times \mathbb{C}^{n_2} \to \mathbb{C}^m$ by setting $B(x, y) := M(xy^t)$ for all $x \in \mathbb{C}^{n_1}, y \in \mathbb{C}^{n_2}$. Throughout the present section we take advantage of this correspondence and work with the set $\mathcal{L}(m)$ of linear maps rather than the set $\mathcal{B}(m)$ of bilinear maps.

Definition III.1. *((s_1, s_2)-injective.) A linear map $M \in \mathcal{L}(m)$ is (s_1, s_2)-injective if $M|_{M^1_{s_1,s_2}(n_1,n_2)}$ is injective.*

Clearly, a bilinear map $B \in \mathcal{B}(m)$ is (s_1, s_2)-injective modulo scaling if and only if the associated linear map $M \in \mathcal{L}(m)$ is (s_1, s_2)-injective.

Let us next introduce a notion of stability for (s_1, s_2)-injective linear maps.

Definition III.2. *(Stability.) A linear map $M \in \mathcal{L}(m)$ is stably (s_1, s_2)-injective if there exists a constant $C > 0$ (possibly dependent on all the parameters of M) such that $\|M(X)\|_2 \geq C\|X\|_F$ for all $X \in \Delta(M^1_{s_1,s_2}(n_1, n_2))$.*

Remark Formally, the notion of stability we give here can be understood as a generalization of the notion of stability given in Definition 2.3 of [30] for the Phase Retrieval Problem. Indeed for $x, y \in \mathbb{R}^n$ we have on the one hand

$$\|x - y\|_2^2\|x + y\|_2^2 - \|xx^t - yy^t\|_F^2 = 2(\|x\|_2^2\|y\|_2^2 - \langle x, y\rangle) \geq 0$$

by the Cauchy-Schwarz inequality and on the other hand

$$\begin{aligned}\|xx^t - yy^t\| = \sup_{\|v\|_2=1} v^t(xx^t - yy^t)v &= \frac{1}{2}\sup_{\|v\|_2=1} v^t((x+y)(x-y)^t + (x-y)(x+y)^t)v \\ &\leq \sup_{\|v\|_2=1,\|u\|_2=1} u^t((x+y)(x-y)^t)v = \|x-y\|_2^2\|x+y\|_2^2,\end{aligned}$$

where $\|\cdot\|$ denotes the operator norm. However, different from [30], throughout the present paper we do not aim for a universal constant C for which the stability bound holds, but rather allow C to depend on all the parameters of the linear map M.

Under the premise of this rather weak notion of stability we obtain the following lower bound on the number of measurement outcomes necessary for (s_1, s_2)-injectivity.

Theorem III.1. *(Lower bound.) If there is a stably (s_1, s_2)-injective linear map $M \in \mathcal{L}(m)$, then*

$$m \geq \begin{cases} 2(n_1 + n_2) - 4 & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1 + s_2) - 2 & \text{else.} \end{cases}$$

The proof of this result can be found in Section IV.

Remark Let us note that this lower bound also applies to a slightly more general scenario which will be of relevance in the next part of this section. Indeed, let $V \subseteq \mathbb{C}^{n_1}$, $W \subseteq \mathbb{C}^{n_2}$ be subspaces with bases $E := \{e_1, \dots, e_{\dim V}\} \subseteq V$ and $F = \{f_1, \dots, f_{\dim W}\} \subseteq W$, respectively. Denote by $V_{s_1} \subseteq V$ the elements of V that are s_1-sparse in the basis E and by $W_{s_2} \subseteq W$ the elements of W that are s_2-sparse in the basis F. If a bilinear map $B \in \mathcal{B}(m)$ is such that B restricted to $V_{s_1} \times W_{s_2}$ is injective modulo scaling, then the bilinear map $\tilde{B} : \mathbb{C}^{\dim V} \times \mathbb{C}^{\dim W} \to \mathbb{C}^n$, $(x, y) \mapsto B(\sum_i x_i e_i, \sum_i y_i f_i)$ is (s_1, s_2)-injective modulo scaling. Thus, under the premise of stability, the lower bound given in III.1 also applies to this scenario.

Next we show that the lower bound given by Theorem III.1 is indeed tight. In the following theorem the term "almost all" refers to the Lebesgue measure on $(M(n_1, n_2))^m$ which represents $\mathcal{L}(m)$ via (1).

Theorem III.2. *(Upper bound.) Almost all linear maps $M \in \mathcal{L}(m)$ are stably (s_1, s_2)-injective if*

$$m \geq \begin{cases} 2(n_1 + n_2) - 4 & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1 + s_2) - 2 & \text{else.} \end{cases}$$

The following Theorem shows that the lower bound established in Theorem III.1 also applies for a certain structured subset of $\mathcal{L}(m)$ which will be of relevance in the next section. In the following theorem the term "almost all" refers to the Lebesgue measure.

Theorem III.3. *For almost all $(Y, Z) \in M(m, n_1) \times M(m, n_2)$, the linear map*

$$M_{Y,Z} : M(n_1, n_2) \to \mathbb{C}^m, \ X \mapsto (tr(Z_1^t Y_1 X), \dots, tr(Z_m^t Y_m X))$$

is stably (s_1, s_2)-injective if

$$m \geq \begin{cases} 2(n_1 + n_2) - 4 & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1 + s_2) - 2 & \text{else.} \end{cases}$$

The proof of this result can be found in Section IV.

B. Blind Deconvolution with Subspace and Sparsity Constraints

In this section we apply Theorem III.3 to the deconvolution problem. By $v \circledast w \in \mathbb{C}^m$ we denote the circular convolution of vectors $v, w \in \mathbb{C}^m$, i.e., for all $i \in \{1, \dots, m\}$ we have $(v \circledast w)_i = \sum_{j=1}^m v_j w_{[(i-j-1) \bmod m]+1}$. The mapping

$$\begin{aligned} C : \mathbb{C}^m \times \mathbb{C}^m &\to \mathbb{C}^m \\ (v, w) &\mapsto v \circledast w \end{aligned}$$

is easily seen to be bilinear. Since the dimension of the domain of C is larger than the dimension of the range of C, C cannot be injective modulo scaling for $m > 1$. However, when imposing sparsity or subspace constraints on the domain of C this can change.

Let us first focus on subspace constraints. For $k \leq m$, consider the set

$$G(m,k) := \{P \in M(m,m) : P \text{ is a rank } k \text{ orthogonal projection.}\}$$

which can naturally be identified with the Grassmannian of k-dimensional subspaces of $\mathbb{C}^m$. We make $(G(m,k), d')$ a compact metric space by setting $d'(P,P') := \|P - P'\|_F$ for all $P, P' \in G(m,k)$. Let μ_k be the Haar measure of $(G(m,k), d')$ with respect to the action $G : U(m) \times G(m,k) \to G(m,k), (U,P) \mapsto UPU^*$ of the unitary group $U(m)$ on $G(m,k)$ [1]. In the following theorem, the term "almost all" refers to the product measure measure $\mu_k \times \mu_l$.

Theorem III.4. *(Deconvolution with subspace constraint.) Let $k, l \in \mathbb{N}_+$ be such that $2(k+l) - 4 \leq m$. Then, for almost all pairs of projections $(P, P') \in G(m,k) \times G(m,l)$, $ran\, P \times ran\, P'$ is strongly identifiable modulo scaling with respect to the circular convolution map $C : \mathbb{C}^m \times \mathbb{C}^m \to \mathbb{C}^m,\ (v,w) \mapsto v \circledast w$.*

Remarks

(a) Note, that this result is optimal. Indeed, since $\Delta(M^1(\dim V, \dim W)) = M^2(\dim V, \dim W)$, we conclude that $\Delta(M^1(\dim V, \dim W))$ is closed. Thus, by Proposition IV.3, the map C restricted to $\operatorname{ran} P \times \operatorname{ran} P$ is injective modulo scaling if and only if the associated linear map $L_C : M(k,l) \to \mathbb{C}^m$ (cf. remark after Theorem III.1) is stably (k,l)-injective. Hence, by Theorem III.1, there do not exist projections $(P, P') \in G(m,k) \times G(m,l)$ such that C restricted to $\operatorname{ran} P \times \operatorname{ran} P'$ is injective modulo scaling if $2(k+l)-4 > m$. This shows the statement for the second part. For the first part the same argument applies.

(b) As a comparison, Theorem 3.2 in [1] requires $2(k+l) < m$ measurements to guarantee strong identifiability, so as expected there is only a small improvement. We hence consider it to be our main achievement that our bounds are provably optimal.

The proof of this theorem is given in Section IV.

Next we consider sparsity constraints. Denote by

$$F(m,k) := \{X \in M(m,k) : \operatorname{rank} X = k\}$$

the set of all collections of k linearly independent vectors in $\mathbb{C}^m$. In the following theorem the term "almost all" refers to the Lebesgue measure.

Theorem III.5. *(Deconvolution with sparsity constraint.) For $E \in F(m,k)$, set $ran(E)_s := \{x \in ran\, E : x \text{ is } s\text{-sparse when expanded in } E.\}$. Let $s_1, s_2 \in \mathbb{N}_+$ be such that $2(s_1+s_2) - 2 \leq m$ and let $k, l \in \mathbb{N}$ be such that $s_1 < k \leq m$, $s_2 < l \leq m$. Then, for almost all pairs $(E, D) \in F(m,k) \times F(m,l)$, $ran(E)_{s_1} \times ran(D)_{s_2}$ is strongly identifiable modulo scaling with respect to the circular convolution map $C : \mathbb{C}^m \times \mathbb{C}^m \to \mathbb{C}^m,\ (v,w) \mapsto v \circledast w$.*

[1] Recall that for (X,d) a compact metric space and G be a group of isometries of (X,d) that acts transitively on X, the Haar measure λ on (X,d) with respect to G is the unique G-invariant Borel measure with $\lambda(X) = 1$ (See for instance theorems 1.1 and 1.3 of [31]).

Remarks

(a) Note that under the premise of stability this result is optimal. Indeed, by Theorem III.1 and the remark afterwards there do not exist $(E, D) \in F(m,k) \times F(m,l)$ such that C restricted to $\mathrm{ran}(E)_{s_1} \times \mathrm{ran}(F)_{s_2}$ is identifiable modulo scaling if $2(s_1+s_2)-2 > m$.

(b) As a comparison, Theorem 3.2 in [1] requires $m > 2(s_1+s_2)$ measurements for strong identifiability in this case.

(c) Note that this result also applies to the standard convolution $\tilde{C} : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^{2n-1}$, $(u,v) \mapsto (\sum_{j=-\infty}^{+\infty} u_j v_{i-(j-1)})_{i=1}^{2n-1}$, where $u_j = 0$, $v_j = 0$ for $j \notin \{1,\dots,n\}$. Indeed, by embedding $\mathbb{C}^n$ appropriately in $\mathbb{C}^{2n-1}$, $\tilde{C}$ can be understood as a restriction of the circular convolution $C : \mathbb{C}^{2n-1} \times \mathbb{C}^{2n-1} \to \mathbb{C}^{2n-1}$.

The proof of this theorem is given in Section IV.

IV. PROOFS

A. Algebraic Geometry Background and Notation

The proof of Theorem III.1 relies on results from classical algebraic geometry so let us fix some conventions (which are close to [32]). We call a set $V \subseteq \mathbb{C}^n$ an algebraic set if it is the common zero locus of a set of complex polynomials in n variables. The Zariski topology on $\mathbb{C}^n$ is defined by choosing its closed sets to be the algebraic sets. A non-empty subset V of $\mathbb{C}^n$ equipped with the Zariski topology is called irreducible if it cannot be expressed as a union of two proper subsets of V, each of which is relatively closed in V. We call an algebraic set an affine variety if it is irreducible. Subsets of an algebraic set that are relatively open in the Zariski topology are called quasi algebraic sets. For a subset $V \subseteq \mathbb{C}^n$, we denote by $P(V) \subseteq P(\mathbb{C}^n)$ its projectification, i.e., the image of V under the canonical projection $P : \mathbb{C}^n \to P(\mathbb{C}^n)$. If a subset $V \subseteq \mathbb{C}^n$ is the common zero locus of a set of homogeneous polynomials, we call $P(V)$ a projective algebraic set. We denote by $\overline{V}$ the analytic closure of a subset $V \subseteq \mathbb{C}^n$, i.e., its closure in the standard topology of $\mathbb{C}^n$. Furthermore $\overline{V}_Z$ denotes the closure of a subset $V \subseteq \mathbb{C}^n$ in the Zariski topology. By $\dim V$ we denote the algebraic dimension of a subset $V \subseteq \mathbb{C}^n$.

For a subset $A \subseteq \{1,\dots,n\}$ define the projection $P_A : \mathbb{C}^n \to \mathbb{C}^n$ by setting

$$(P_A(x))_i := \begin{cases} x_i & \text{if } i \in A, \\ 0 & \text{else} \end{cases}$$

for all $x \in \mathbb{C}^n$ and $i \in \{1,\dots,n\}$. Furthermore, let $\mathcal{A}(n,s) := \{A \subseteq \{1,\dots,n\} : |A| = s\}$. Then

$$M^1_{s_1,s_2}(n_1,n_2) = \bigcup_{A \in \mathcal{A}(n_1,s_1),\ B \in \mathcal{A}(n_2,s_2)} W_{A,B},$$

where $W_{A,B} := \{P_A u (P_B v)^* : u \in \mathbb{C}^{n_1},\ v \in \mathbb{C}^{n_2}\}$. Let $S_{s_1,s_2} := W_{\{1,\dots,s_1\},\{1,\dots,s_2\}}$.

B. Proof of Theorem III.1

Theorem III.1 can be proven straightforwardly from the following three propositions. Their proofs are relegated to the end of this subsection.

Proposition IV.1. *We have*

$$\dim \Delta(M^1_{s_1,s_2}(n_1,n_2)) = \begin{cases} 2(n_1+n_2-2) & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1+s_2-1) & \text{else.} \end{cases}$$

Proposition IV.2. *The analytic closure of $\Delta(M^1_{s_1,s_2}(n_1,n_2))$ is the common zero locus of a set of homogeneous polynomials. In particular $\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))} = \overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))}_Z$.*

Proposition IV.3. *A linear map $M \in \mathcal{L}(m)$ is stably (s_1,s_2)-injective if and only if $P(\ker M) \cap P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))}) = \emptyset$.*

Proof of Theorem III.1. By Proposition IV.3 a linear map $M \in \mathcal{L}(m)$ is stably (s_1,s_2)-injective if and only if $P(\ker M) \cap P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))}) = \emptyset$. Clearly $P(\ker M)$ is a projective algebraic set and by Proposition IV.2, $P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))})$ also is a projective algebraic set.

By the intersection theorem for complex varieties (see Theorem 7.2 of [32]), together with the observation that a projective algebraic set contains an irreducible projective algebraic subset of the same dimension, two projective algebraic sets $V, W \subseteq P(\mathbb{C}^{n+1})$ have non-empty intersection if $\dim V + \dim W \geq n$. Hence, if M is stably (s_1,s_2)-injective we have $\dim P(\ker M) + \dim P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))}) < \dim P(\mathbb{C}^{n_1 n_2})$. Noting that $\dim P(\ker M) \geq n_1 n_2 - m - 1$ [2], we find $n_1 n_2 - m - 1 + \dim P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))}) < n_1 n_2 - 1$. But this implies, using again Proposition IV.2, that

$$\begin{aligned} m &\geq \dim P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))}) + 1 = \dim \overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))} \\ &= \dim \overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))}_Z = \dim \Delta(M^1_{s_1,s_2}(n_1,n_2)) \end{aligned}$$

and Proposition IV.1 concludes the proof. □

Proof of Proposition IV.1. Let $A \in \mathcal{A}(n_1,s_1)$, $B \in \mathcal{A}(n_2,s_2)$. We begin by determining the dimension of $W_{A,B}$. $W_{A,B}$ is the set of $X \in M^1(n_1,n_2)$ such that $((\mathbb{1}_{n_1} - P_A)X)_{ij} = 0$, $(X(\mathbb{1}_{n_2} - P_B))_{ij} = 0$ for all $i \in \{1,\ldots,n_1\}$, $j \in \{1,\ldots,n_2\}$. Furthermore, $M^1(n_1,n_2)$ is well-known to be an algebraic set [3] and hence $W_{A,B}$ is an algebraic set. Let $I_A : \mathbb{C}^{s_1} \to \operatorname{ran} P_A$, $I_B : \mathbb{C}^{s_2} \to \operatorname{ran} P_B$ be the canonical linear embeddings, then the mapping

$$\eta : M(s_1,s_2) \to W_{A,B},\ X \to I_A X I_B \tag{2}$$

also is a linear embedding. In particular $\eta|_{M^1(s_1,s_2)}$ yields an isomorphism between $M^1(s_1,s_2)$ and $W_{A,B}$. Hence, using Example 12.1 of [33], we find $\dim W_{A,B} = \dim M^1(s_1,s_2) = s_1 + s_2 - 1$.

---

[2] Note that if $V \subseteq \mathbb{C}^n$ is such that $P(V)$ is a projective algebraic set, then $\dim P(V) = \dim V - 1$.

[3] $M^1(n_1,n_2)$ is the common zero locus of the 2×2-minors.

We now start by considering the case $n_1 = s_1$ and $n_2 = s_2$. In this case we find $\Delta(M^1_{n_1,n_2}(n_1,n_2)) = \Delta(M^1(n_1,n_2)) = M^2(n_1,n_2)$. The set $M^2(n_1,n_2)$ is an algebraic set and its dimension is given by $2(n_1+n_2-2)$ (Again by Example 12.1 of [33].).

Secondly, let us assume that $s_1 < n_1$, the case $s_2 < n_2$ can be treated analogously. Let $A, A' \in \mathcal{A}(n_1,s_1),\ B, B' \in \mathcal{A}(n_2,s_2)$. Consider the morphism

$$\begin{aligned}\psi : W_{A,B} \times W_{A',B'} &\to M(n_1,n_2)\\ (X,Y) &\to X - Y\end{aligned}$$

and note that $\psi(W_{A,B} \times W_{A',B'}) = W_{A,B} - W_{A',B'}$. Therefore we find

$$\dim(W_{A,B} - W_{A',B'}) \leq \dim W_{A,B} + \dim W_{A',B'} = 2\dim S = 2(s_1+s_2-1)$$

and since $\Delta(M^1_{s_1,s_2}(n_1,n_2)) = \bigcup_{A,A' \in \mathcal{A}(n_1,s_1),\ B,B' \in \mathcal{A}(n_2,s_2)} W_{A,B} - W_{A',B'}$ this implies

$$\dim \Delta(M^1_{s_1,s_2}(n_1,n_2)) \leq 2(s_1+s_2-1). \tag{3}$$

Since $s_1 < n_1$ there exist $A, A' \in \mathcal{A}(n_1,s_1)$ such that $1 \in A$, $1 \notin A'$ and $2 \in A'$, $2 \notin A$. Furthermore, let $B \in \mathcal{A}(n_2,s_2)$ and consider the set

$$\begin{aligned}\mathcal{D} :=& W_{A,B} \times W_{A',B} \cap \{(X,Y) \in M(n_1,n_2) \times M(n_1,n_2) : X_{11} \neq 0,\ Y_{21} \neq 0,\\ & Y_{21} \cdot X_1 - X_{11} \cdot Y_2 \neq 0\}.\end{aligned}$$

The set $\mathcal{D}$ clearly is non-empty and quasi algebraic. Furthermore we have $\dim \mathcal{D} = 2(s_1 + s_2 - 1)$. One way to see this is the following: Since both $W_{A,B}$ and $W_{A',B}$ are isomorphic to $M^1(s_1,s_2)$, $W_{A,B} \times W_{A',B}$ is isomorphic to $M^1(s_1,s_2) \times M^1(s_1,s_2)$. By Proposition 12.2 of [33] $M^1(s_1,s_2)$ is irreducible [4] and hence an affine variety. By Exercice 3.15 of [32], the product of two affine varieties is irreducible and hence $M^1(s_1,s_2) \times M^1(s_1,s_2)$ is irreducible. Finally, by Example 1.1.3 of [32] a non-empty quasi algebraic subset of an irreducible set is irreducible. Hence $\mathcal{D}$ is irreducible and thus by Exercise 1.6 and Proposition 1.10 of [32] we have $\dim \mathcal{D} = \dim \overline{\mathcal{D}}_Z = \dim W_{A,B} \times W_{A',B} = 2(s_1+s_2-1)$ [5].

Next we prove that $\dim \psi(\mathcal{D}) = \dim \mathcal{D} = 2(s_1+s_2-1)$ by showing that the morphism $\psi|_{\mathcal{D}}$ is injective: Let $(X,Y) \in \mathcal{D}$. Then, by the definition of $\mathcal{D}$, X_1 and Y_2 are non-vanishing and linearly independent. Hence there are vectors $\omega_1(X), \omega_2(Y) \in \mathbb{C}^{n_2}$ such

---

[4] Proposition 12.2 of [33] just states that $P(M^1(s_1,s_2))$ is irreducible. An algebraic set is irreducible if and only if its associated polynomial ideal is prime and the same holds for projective algebraic sets (see for instance Corollary 1.4 and Exercise 2.4 (b) of [32]). But the polynomial ideals associated to $PM^1(s_1,s_2)$ and $M^1(s_1,s_2)$ clearly are equal and thus $M^1(s_1,s_2)$ is irreducible as well.

[5] A more direct approach consists of showing the injectivity of the mapping

$$\begin{aligned}&(\mathbb{C}^{s_1} \setminus \{0\} \times \mathbb{C}^{s_2-1} \setminus \{0\}) \times (\mathbb{C}^{s_1} \setminus \{0\} \times \mathbb{C}^{s_2-1} \setminus \{0\}) \setminus \mathcal{S} \to \mathcal{D},\\ &((u,v),(u',v')) \mapsto \left(I_A(u) I_B \left(\begin{pmatrix} 1 \\ v \end{pmatrix} \right)^t, I_{A'}(u') I_B \left(\begin{pmatrix} 1 \\ v' \end{pmatrix} \right)^t \right)\end{aligned}$$

where $\mathcal{S} := \{((u,v),(u',v')) \in (\mathbb{C}^{s_1} \setminus \{0\} \times \mathbb{C}^{s_2-1} \setminus \{0\}) \times (\mathbb{C}^{s_1} \setminus \{0\} \times \mathbb{C}^{s_2-1} \setminus \{0\}) : v_1 - v'_1 = 0,\ u_1 = 0,\ u'_2 = 0\}$ and I_A denotes a linear embedding of $\mathbb{C}^s_1$ into $\operatorname{ran} P_A$. We leave details to the reader.

that $\langle \omega_1(X), X_1 \rangle = 1$, $\langle \omega_2(Y), X_1 \rangle = 0, \langle \omega_1(X), Y_2 \rangle = 0$ and $\langle \omega_2(Y), Y_2 \rangle = 1$. Note that $\langle \omega_1(X), Y_i \rangle = 0$ for all $i \in \{1, \dots, n_1\}$ by the fact that Y is rank one. Similarly we have $\langle \omega_2(Y), X_i \rangle = 0$ for all $i \in \{1, \dots, n_1\}$. Again using the fact that both X and Y are rank one it follows from a straightforward computation that for all $i \in \{1, \dots, n_1\}$ we have

$$\begin{aligned} \langle \omega_1(X), (X-Y)_i \rangle X_1 &= \langle \omega_1(X), X_i \rangle X_1 = X_i \\ -\langle \omega_2(Y), (X-Y)_i \rangle Y_2 &= \langle \omega_2(Y), Y_i \rangle Y_2 = Y_i. \end{aligned}$$

This explicitly defines an inverse map of ψ on $\psi(\mathcal{D})$, showing that $\psi|_D$ is injective.

But since $\psi(D) \subseteq \Delta(M^1_{s_1,s_2}(n_1,n_2)) = \bigcup_{A,A' \in \mathcal{A}(n_1,s_1),\ B,B' \in \mathcal{A}(n_2,s_2)} W_{A,B} - W_{A',B'}$ we find $2(s_1+s_2-1) = \dim \mathcal{D} = \dim \psi(D) \leq \dim \Delta(M^1_{s_1,s_2}(n_1,n_2))$, which, together with Inequality (3), concludes the proof. □

Proof of Proposition IV.2. Since

$$\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))} = \bigcup_{A,A' \in \mathcal{A}(n_1,s_1),\ B,B' \in \mathcal{A}(n_2,s_2)} \overline{W_{A,B} - W_{A',B'}},$$

it suffices to prove that $\overline{W_{A,B} - W_{A',B'}}$ is the common zero locus of a set of homogeneous polynomials for all $A, A' \in \mathcal{A}(n_1, s_1),\ B, B' \in \mathcal{A}(n_2, s_2)$.

So let $A, A' \in \mathcal{A}(n_1, s_1),\ B, B' \in \mathcal{A}(n_2, s_2)$. By the first paragraph in the proof of Theorem 3.16 of [33], $\psi(W_{A,B} \times W_{A',B'}) = W_{A,B} - W_{A',B'} \subseteq M(n_1, n_2)$ contains a non-empty quasi algebraic subset of its Zarisiki closure [6]. Consequently, the analytic closure of $W_{A,B} - W_{A',B'}$ coincides with its Zariski closure by Theorem 1 in Chapter 1.10 of [34]. Hence the analytic closure of $W_{A,B} - W_{A',B'}$ is the common zero locus of a finite set of polynomials $\{p_i\}_{i \in I}$.

Let $X \in \overline{W_{A,B} - W_{A',B'}}$. We now show that $\lambda X \in \overline{W_{A,B} - W_{A',B'}}$ for all $\lambda \in \mathbb{C}$: There exists a sequence $(X_n)_{n \in \mathbb{N}} \subseteq W_{A,B} - W_{A',B'}$ that converges to X. Next observe that if $Y \in W_{A,B} - W_{A',B'}$ we also have $\lambda Y \in W_{A,B} - W_{A',B'}$ for all $\lambda \in \mathbb{C}$. Now let $\lambda \in \mathbb{C}$ and observe that the sequence $(\lambda X_n)_{n \in \mathbb{N}} \subseteq W_{A,B} - W_{A',B'}$ converges to λX and thus $\lambda X \in \overline{W_{A,B} - W_{A',B'}}$.

Finally we just have to show that $\overline{W_{A,B} - W_{A',B'}}$ is the common zero locus of a set of homogeneous polynomials. Let $i \in I$ and let d_i be the degree of p_i. Consider the decomposition $p_i = \sum_{j=0}^{d_i} p_{i,j}$ where the $p_{i,j}$ are homogeneous polynomials of degree j. Let $X \in \overline{W_{A,B} - W_{A',B'}}$. Then we have for all $\lambda \in \mathbb{C}$

$$0 = p_i(\lambda X) = \sum_{j=0}^{d} \lambda^j p_{i,j}(X).$$

Since this holds for all $\lambda \in \mathbb{C}$, we conclude that $p_i(X) = 0$ if and only if $p_{i,j}(X) = 0$ for all $j \in \{1, \dots, d\}$. Repeating this for all $i \in I$ we find a set $J := \{p_{i,j}\}_{i \in I, j \in \{1,\dots,d_i\}}$ of homogenous polynomials such that $\overline{W_{A,B} - W_{A',B'}}$ is the common zero locus of J. □

[6] Here, we use the fact that $\mathbb{C}^n$ is homeomorphic to $P(\mathbb{C}^{n+1}) \setminus \{x_0 = 0\}$ (See Proposition 2.2 in [32].).

Proof of Proposition IV.3. Assume for a contradiction that there is $X \in M(n_1, n_2)$ with $\|X\|_F = 1$ such that $P(X) \in P(\ker M) \cap P(\overline{\Delta(M^1_{s_1,s_2}(n_1, n_2))})$. Then there is a sequence $(X_n)_{n\in\mathbb{N}} \subseteq \Delta(M^1_{s_1,s_2}(n_1, n_2))$ with $\|X_n\|_F = 1$ for all $n \in \mathbb{N}$ that converges to X. Thus, by the continuity of M, the sequence $\|M(X_n)\|_2$ converges to $\|M(X)\|_2 = 0$. In particular for any $c > 0$ there is an $N \in \mathbb{N}$ such that $\|M(X_N)\|_2 \leq c$.

Conversely set $C = \min_{Y\in O} \|M(Y)\|_2$ where $O := \{Y \in \overline{\Delta(M^1_{s_1,s_2}(n_1, n_2))} : \|Y\|_F = 1\}$. If $P(\ker M) \cap P(\overline{\Delta(M^1_{s_1,s_2}(n_1, n_2))}) = \emptyset$ we have $\|M(Y)\|_2 > 0$ for all $Y \in O$ and by compactness of O we conclude $C > 0$. □

C. Proofs of Theorems III.2 and III.3

The approach we take in this section is similar to the approach taken in [35] to prove injectivity for the phase retrieval problem. The proofs of the theorems are immediate consequence of the following two proposition. Their proof is very close to the proof of Proposition III.1 in [36].

Proposition IV.4. *Let*

$$m \geq \begin{cases} 2(n_1 + n_2) - 4 & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1 + s_2) - 2 & \text{else.} \end{cases} \tag{4}$$

Then, the set of $(Y, Z) \in M(m, n_1) \times M(m, n_2)$ *such that the linear map*

$$M_{Y,Z} : M(n_1, n_2) \to \mathbb{C}^m,\ X \mapsto (tr(Z_1^t Y_1 X), \ldots, tr(Z_m^t Y_m X))$$

is not stably (s_1, s_2)*-injective has strictly smaller dimension than the set* $M(m, n_1) \times M(m, n_2)$.

Remark This proposition directly implies Theorem III.3.

Proof. Consider the quasi algebraic set

$$\mathcal{W} := \bigcup_{i\in\{1,\ldots,n_1\}, j\in\{1,\ldots,n_2\}} \overline{\Delta(M^1_{s_1,s_2}(n_1, n_2))} \cap \{X \in M(n_1, n_2) : X_{ij} = 1\}.$$

Intuitively, the set $\mathcal{W}$ is the union of the canonical charts of $P(\overline{\Delta(M^1_{s_1,s_2}(n_1, n_2))})$ and hence we find $P(\mathcal{W}) = P(\overline{\Delta(M^1_{s_1,s_2}(n_1, n_2))})$ and furthermore, using Proposition IV.1,

$$\dim \mathcal{W} = \dim P(\overline{\Delta(M^1_{s_1,s_2}(n_1, n_2))}) = \dim \Delta(M^1_{s_1,s_2}(n_1, n_2)) - 1 < m.$$

For $(Y, Z) \in M(m, n_1) \times M(m, n_2)$ and $X \in M(n_1, n_2)$ define the polynomials

$$p_i(Y, Z, X) := \operatorname{tr}(Z_i^t Y_i X),\ i \in \{1, \ldots, m\}. \tag{5}$$

By $\mathcal{V}$ we denote the common zero locus of the polynomials $\{p_i\}_{i\in\{1,\ldots,m\}}$. Now consider the algebraic set

$$\mathcal{D} := (M(m, n_1) \times M(m, n_2) \times \mathcal{W}) \cap \mathcal{V}$$

and let $\pi : M(m,n_1) \times M(m,n_2) \times \mathcal{W} \to M(m,n_1) \times M(m,n_2)$ be the projection on the factor $M(m,n_1) \times M(m,n_2)$. Let

$$\mathcal{N} := \{(Y,Z) \in M(m,n_1) \times M(m,n_2) : M_{Y,Z} \text{ is not stably } (s_1,s_2)\text{-injective.}\},$$

then we have $\mathcal{N} \subseteq \pi(\mathcal{D})$ [7]. Indeed, let $(Y,Z) \in \mathcal{N}$. Then, by Proposition IV.3, there exists $Q \in P(\ker M_{Y,Z}) \cap P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))})$. Since $P(\mathcal{W}) = P(\overline{\Delta(M^1_{s_1,s_2}(n_1,n_2))})$, there exists an $X \in \mathcal{W}$ such that $P(X) = Q$. But then, by linearity of $M_{Y,Z}$, we have $M_{Y,Z}(X) = 0$, i.e., $(Y,Z,X) \in \mathcal{D}$. Consequently we have $(Y,Z) \in \pi(\mathcal{D})$.

We will assume for now and show later that $\dim \mathcal{D} = \dim M(m,n_1) + \dim M(m,n_2) + \dim \mathcal{W} - m$. Then, using $m > \dim \mathcal{W}$, we find that

$$\begin{aligned}\dim \pi(\mathcal{D}) &\leq \dim \mathcal{D} = \dim M(m,n_1) + \dim M(m,n_2) + \dim \mathcal{W} - m \\ &< \dim M(m,n_1) + \dim M(m,n_2).\end{aligned}$$

That is, $\pi(\mathcal{D}) \subseteq M(m,n_1) \times M(m,n_2)$ has strictly smaller dimension than $M(m,n_1) \times M(m,n_2)$ (and thus has Lebesgue measure zero in $M(m,n_1) \times M(m,n_2)$).

Hence, to conclude the proof, it suffices to show that indeed $\dim \mathcal{D} = \dim M(m,n_1) + \dim M(m,n_2) + \dim \mathcal{W} - m$. To show this, it suffices to prove that for fixed $X \in \mathcal{W}$ the equations $\{p_i = 0\}_{i \in \{1,\dots,m\}}$ reduce the dimension of $M(m,n_1) \times M(m,n_2)$ by m (cf. [35]). But for fixed $X \in \mathcal{W}$, the i-th equation of (5) just involves the variables of the i-th factor of $(\mathbb{C}^{n_1} \times \mathbb{C}^{n_2})^m \simeq M(m,n_1) \times M(m,n_2)$. Hence it suffices to prove that for fixed $X \in \mathcal{W}$ the equation

$$\operatorname{tr}(vw^t X) = 0,\ v \in \mathbb{C}^{n_2}, w \in \mathbb{C}^{n_1}, \tag{6}$$

reduces the dimension of $\mathbb{C}^{n_1} \times \mathbb{C}^{n_2}$ by one. But Equation (6) is a non-trivial algebraic equation on $\mathbb{C}^{n_1} \times \mathbb{C}^{n_2}$ because $X \neq 0$ and $M(n_1,n_2)$ has a basis of rank one operators. Hence, by Proposition 1.13 of [32], Equation (6) reduces the dimension of $\mathbb{C}^{n_1} \times \mathbb{C}^{n_2}$ by one. □

Proposition IV.5. *Let*

$$m \geq \begin{cases} 2(n_1+n_2)-4 & \text{if } s_1 = n_1, s_2 = n_2, \\ 2(s_1+s_2)-2 & \text{else.} \end{cases}$$

Then, the set of $Y := (Y_1,\dots,Y_m) \in (M(n_2,n_1))^m$ *such that the linear map*

$$M_Y : M(n_1,n_2) \to \mathbb{C}^m,\ X \mapsto (tr(Y_1X),\dots,tr(Y_mX))$$

is not stably (s_1,s_2)*-injective has smaller dimension than the set* $(M(n_n,n_1))^m$.

Remark This proposition directly implies Theorem III.2.

[7] We even have $\mathcal{N} = \pi(\mathcal{D})$. This, however, will not be of relevance for our argument.

Proof. Instead of the polynomials defined in Equation (5), now consider the polynomials

$$q_i(Y, X) := \mathrm{tr}(Y_i X),\ i \in \{1, \ldots, m\}$$

in $(Y_1, \ldots, Y_m) \in (M(n_2, n_1))^m$ and $X \in M(n_1, n_2)$.

All the arguments given in the remainder of the proof of Proposition IV.4 are also valid for these polynomials. Thus the proof can be concluded by going along the lines of the proof of Proposition IV.4. □

D. Proof of theorems III.4 and III.5

Denote by $F := \left(\frac{1}{\sqrt{m}} e^{2i\pi \frac{kl}{m}}\right)_{k,l=1}^{m} \in M(m, m)$ the discrete Fourier matrix. Then we have the following well-known identity

$$v \circledast w = mF^* \left((Fv) \odot (Fw)\right), \forall v, w \in \mathbb{C}^m, \tag{7}$$

where $\odot$ denotes the Hadamard product, i.e., for $a, b \in \mathbb{C}^m$ we have $a \odot b = (a_i b_i)_{i=1}^m$.

Proof of Theorem III.5. Since F is invertible it suffices to show that the map $C' : \mathbb{C}^k \times \mathbb{C}^l \to \mathbb{C}^m,\ (u, v) \mapsto (FEu) \odot (FDv)$ is injective modulo scaling for Lebesgue almost all $(E, D) \in M(m, k) \times M(m, l)$. Let $u \in \mathbb{C}^k$, $v \in \mathbb{C}^l$ and $(E, D) \in M(m, k) \times M(m, l)$, then

$$(C'(u, v))_i = (FEu)_i (FDv)_i = e_i^t FEuv^t D^t F^t e_i = \mathrm{tr}\left([(FD)_i]^t (FE)_i uv^t\right),$$

where $\{e_i\}_{i \in \{1, \ldots, m\}}$ denotes the standard orthonormal basis of $\mathbb{C}^m$. Theorem III.4 implies that C' is injective modulo scaling for Lebesgue almost all $(FE, FD) \in M(m, k) \times M(m, l)$ and hence, since the Lebesgue measure λ is unitarily invariant, also for Lebesgue almost all $(E, D) \in M(m, k) \times M(m, l)$. □

Finally, the proof of Theorem III.4 proceeds identically as the proof of Theorem III.5. It only remains to check that in the process of converting the statement of Theorem III.5 into a statement about the Haar measure on Grassmannians, the set $\mathcal{I} := \{(E, D) \in M(m, k) \times M(m, l) : C' \text{ is injective modulo scaling.}\}$ is mapped to a full measure set. However, since this part of the argument is mainly technical, we relegate it to Appendix A.

Acknowledgements

We thank Kiryung Leee and Dustin Mixon for helpful comments. This work was inspired by the workshop Frames and Algebraic & Combinatorial Geometry at the University of Bremen. F.K.'s contribution was supported by the German Science Foundation (DFG) in the context of the Emmy Noether Junior Research Group 'Randomized Sensing and

Quantization of Signals and Images" (KR 4512/1-1) and the project "Bilinear Compressed Sensing" (KR 4512/2-1).

---

[1] Yanjun Li, Kiryung Lee, and Yoram Bresler. Identifiability in blind deconvolution under minimal assumptions. preprint, arXiv:1507.01308, 2015.

[2] E. Candès, J. Romberg, and T. Tao. Stable signal recovery from incomplete and inaccurate measurements. *Comm. Pure Appl. Math*, 59(8):1207–1223, 2006.

[3] D.L. Donoho. Compressed sensing. *IEEE Trans. Inform. Theory*, 52(4):1289 –1306, 2006.

[4] Simon Foucart and Holger Rauhut. *A Mathematical Introduction to Compressive Sensing*. Applied and Numerical Harmonic Analysis. Birkhäuser, 2013.

[5] V. Chandrasekaran, Benjamin Recht, P.A. Parrilo, and Alan S. Willsky. The convex geometry of linear inverse problems. *Found. Comput. Math.*, 12(6):805–849, 2012.

[6] Boris Alexeev, Jameson Cahill, and Dustin G. Mixon. Full spark frames. *J. Fourier Anal. Appl.*, 18(6):1167–1194, 2012.

[7] Yonina C Eldar, Deanna Needell, and Yaniv Plan. Uniqueness conditions for low-rank matrix recovery. *Appl. Comp. Harmon. Anal.*, 33(2):309–314, 2012.

[8] Erwin Riegler, David Stotz, and Helmut Bölcskei. Information-theoretic limits of matrix completion. In *Proc. IEEE Intl. Symposium Inform. Theory (ISIT)*, pages 1836–1840, 2015.

[9] Emmanuel J. Candès, Thomas Strohmer, and Vladislav Voroninski. Phaselift: exact and stable signal recovery from magnitude measurements via convex programming. *Commun. Pure Appl. Math.*, 66(8):1241–1274, 2013.

[10] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Appl. Comput. Harmon. Anal.*, 20(3):345–356, 2006.

[11] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. *Appl. Comp. Harmon. Anal.*, 38(2):346–356, 2015.

[12] Cynthia Vinzant. A small frame and a certificate of its injectivity. *preprint*, 2015.

[13] Kiryung Lee, Yihong Wu, and Yoram Bresler. Near optimal compressed sensing of sparse rank-one matrices via sparse power factorization. *arXiv preprint arXiv:1312.0525*, 2013.

[14] Yanjun Li, Kiryung Lee, and Yoram Bresler. A unified framework for identifiability analysis in bilinear inverse problems with applications to subspace and sparsity models. preprint, arXiv:1501.06120, 2015.

[15] F. Krahmer and H. Rauhut. Structured random measurements in signal processing. *GAMM-Mitteilungen*, 37(2):217–238, 2014.

[16] M. Rudelson and R. Vershynin. On sparse reconstruction from Fourier and Gaussian measurements. *Comm. Pure Appl. Math.*, 61:1025–1045, 2008.

[17] M. Lustig, D. Donoho, and J.M. Pauly. Sparse MRI: The application of compressed sensing for rapid MRI imaging. *Magnetic Resonance in Medicine*, 58(6):1182–1195, 2007.

[18] F. Krahmer, S. Mendelson, and H. Rauhut. Suprema of chaos processes and the restricted isometry property. *Comm. Pure Appl. Math.*, 67(11):1877–1904, 2014.

[19] Roummel F Marcia and Rebecca M Willett. Compressive coded aperture superresolution image reconstruction. In *IEEE Intl. Conf. Acoustics, Speech and Signal Proc. (ICASSP) 2008*, pages 833–836. IEEE, 2008.

[20] Emmanuel J. Candès and Benjamin Recht. Exact matrix completion via convex optimization. *Found. Comput. Math.*, 9:717–772, 2009.

[21] Afonso S Bandeira, Yutong Chen, and Dustin G Mixon. Phase retrieval from power spectra of masked signals. *Inform. Inference*, 3(3):83–102, 2014.

[22] Emmanuel J Candes, Xiaodong Li, and Mahdi Soltanolkotabi. Phase retrieval from coded

diffraction patterns. *Applied and Computational Harmonic Analysis*, 39(2):277–299, 2015.
[23] D. Gross, F. Krahmer, and R. Küng. Improved recovery guarantees for phase retrieval from coded diffraction patterns. *Appl. Comput. Harmon. Anal.*, to appear.
[24] Shuyang Ling and Thomas Strohmer. Self-calibration and biconvex compressive sensing. *Inverse Problems*, 31(11):115002, 2015.
[25] Ali Ahmed, Benjamin Recht, and Justin Romberg. Blind deconvolution using convex programming. *IEEE Trans. Inform. Theory*, 60(3):1711–1732, 2014.
[26] Shuyang Ling and Thomas Strohmer. Blind deconvolution meets blind demixing: Algorithms and performance bounds. preprint, arXiv:1512.07730, 2015.
[27] Sunav Choudhary and Urbashi Mitra. Identifiability scaling laws in bilinear inverse problems. preprint, arXiv:1402.2637, 2014.
[28] Shobhit Choudhary and Urbashi Mitra. Sparse blind deconvolution: What cannot be done. In *IEEE Intl. Symp. Inform. Theory (ISIT)*, pages 3002–3006. IEEE, 2014.
[29] Yanjun Li, Kiryung Lee, and Yoram Bresler. Identifiability in blind deconvolution with subspace or sparsity constraints. preprint, arXiv:1505.03399, 2015.
[30] Yonina C Eldar and Shahar Mendelson. Phase retrieval: Stability and recovery guarantees. *Applied and Computational Harmonic Analysis*, 36(3):473–494, 2014.
[31] Vitali D Milman and Gideon Schechtman. *Asymptotic Theory of Finite Dimensional Normed Spaces: Isoperimetric Inequalities in Riemannian Manifolds*, volume 1200. Springer, 2009.
[32] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 1977.
[33] Joe Harris. *Algebraic geometry: a first course*, volume 133. Springer Science & Business Media, 2013.
[34] David Mumford. *The red book of varieties and schemes: includes the Michigan lectures (1974) on curves and their Jacobians*, volume 1358. Springer Science & Business Media, 1999.
[35] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Applied and Computational Harmonic Analysis*, 20(3):345–356, 2006.
[36] Michael Kech and Michael M. Wolf. Quantum tomography of semi-algebraic sets with constrained measurements. preprint, arXiv:1507.00903, 2015.

APPENDIX A: COMPLETITION OF THE PROOF OF THEOREM III.4

Let $S(m,k) := \{Y \in M(m,k) : \|Y\|_F = 1\} \subseteq M(m,k)$ be the unit sphere in $M(m,k)$. We make $(S(m,k),d)$ a compact metric space by setting $d(X,Y) := \|X-Y\|_F$ for all $X,Y \in S(m,k)$. Let $U(m,k)$ be the group of isometries of $(S(m,k),d)$ and let σ_k be the Haar measure on $S(m,k)$ with respect to $U(m,k)$. Let

$$\pi_k : M(m,k) \setminus \{0\} \to S(m,k),\ X \mapsto \frac{X}{\|X\|_F}.$$

Furthermore let $\pi : M(m,k) \setminus \{0\} \times M(m,l) \setminus \{0\} \to S(m,k) \times S(m,l),\ (X,Y) \mapsto (\pi_k(X), \pi_l(Y))$. It is well-known that for all Borel sets $A \in \mathcal{B}(S(m,k))$ we have $\sigma_k(A) = \lambda(\pi_k^{-1}(A) \cap B_{m,k})/\lambda(B_{m,k})$ where $B_{m,k} = \{X \in M(m,k) : \|X\|_F \leq 1\}$ is the unit ball in $M(m,k)$. But the mapping $\pi : M(m,k) \setminus \{0\} \times M(m,l) \setminus \{0\} \to S(m,k) \times S(m,l),\ (X,Y) \mapsto (X/\|X\|_F, Y/\|Y\|_F)$ maps the set $\mathcal{I}$ of full measure in λ to the set $\pi(\mathcal{I})$ of full measure in $\sigma_k \times \sigma_l$. Indeed, since $\pi^{-1}(\pi(\mathcal{I})) = \bigcup_{\nu>0} \nu\mathcal{I} = \mathcal{I}$ and

$(\lambda \times \lambda)(\mathcal{I}^c) = 0$, we find

$$(\sigma_k \times \sigma_l)(\pi(\mathcal{I})) = \frac{(\lambda \times \lambda)\left(\pi^{-1}(\pi(\mathcal{I})^c) \cap (B_{m,k} \times B_{m,l})\right)}{\lambda(B_{m,k})\lambda(B_{m,l})}$$
$$= \frac{(\lambda \times \lambda)\left(\pi^{-1}(\pi(\mathcal{I}))^c \cap (B_{m,k} \times B_{m,l})\right)}{\lambda(B_{m,k})\lambda(B_{m,l})} = \frac{(\lambda \times \lambda)\left(\mathcal{I}^c \cap (B_{m,k} \times B_{m,l})\right)}{\lambda(B_{m,k})\lambda(B_{m,l})} = 0.$$

Let $S_k(m,k) := \{X \in S(m,k) : \operatorname{rank} X = k\}$ and consider the continuous mapping

$$\begin{aligned} \varphi_k : S_k(m,k) &\to G(m,k) \\ X &\mapsto \Pi_{\operatorname{ran} X}. \end{aligned} \tag{A1}$$

where $\Pi_{\operatorname{ran} X}$ denotes the orthogonal projection on $\operatorname{ran} X$. Furthermore let $\varphi : S_k(m,k) \times S_l(m,l) \to G(m,k) \times G(m,l)$, $(X,Y) \mapsto (\varphi_k(X), \varphi_l(Y))$. Observe that $\varphi(\pi(\mathcal{I}))$ is precisely the set of $(P,P') \in G(m,k) \times G(m,l)$ such that $C|_{\operatorname{ran} P \times \operatorname{ran} P'}$ is injective modulo scaling. We define a measure $\tilde{\mu}_k$ on $G(m,k)$ by setting $\tilde{\mu}_k(A) := \sigma_k(\varphi_k^{-1}(A))$ for all Borel subsets $A \in \mathcal{B}(G(m,k))$. From this one can seen that in the measure $\tilde{\mu}_k \times \tilde{\mu}_l$, the set $\varphi(\pi(\mathcal{I}))$ [8] has full measure and hence the following proposition concludes the proof of Theorem III.4.

Proposition A.1. *The measure $\tilde{\mu}_k$ coincides with the the Haar measure μ_k on $G(m,k)$.*

Proof. First note that $\tilde{\mu}_k(G(m,k)) = \sigma_k(\varphi^{-1}(G(m,k))) = \sigma_k(S_k(m,k)) = 1$. Hence it suffices to check that $\tilde{\mu}(UAU^*) = \tilde{\mu}(A)$ for all $U \in U(m)$ and $A \in \mathcal{B}(G(m,k))$. Let $U \in U(m)$ and $A \in \mathcal{B}(G(m,k))$. Then, since $U(m)S_k(m,k) = S_k(m,k)$,

$$\begin{aligned} \tilde{\mu}_k(UAU^*) &= \sigma_k(\{X \in S_k(m,k) : \Pi_{\operatorname{ran} X} \in UAU^*\}) \\ &= \sigma_k(\{X \in S_k(m,k) : U^*\Pi_{\operatorname{ran} X}U \in A\}) \\ &= \sigma_k(\{X \in S_k(m,k) : \Pi_{\operatorname{ran} U^*X} \in A\}) \\ &= \sigma_k(U\{X \in S_k(m,k) : \Pi_{\operatorname{ran} X} \in A\}) \\ &= \sigma_k(\{X \in S_k(m,k) : \Pi_{\operatorname{ran} X} \in A\}), \end{aligned}$$

where we used the unitary invariance of σ in the last step. □

APPENDIX B: WEAK IDENTIFIABILITY CONDITIONS FOR DECONVOLUTION MAPS

In this appendix we apply the techniques used in the present paper to the weak identifiability problem, achieving a small improvement with respect to Theorem 3.1 in [1] (which agrees with our result except that a strict inequality $m > s_1 + s_2$ is required) and showing optimality of the resulting bound. As the proofs are in large parts very similar to those of our main results, we omit some details.

[8] Note that $\varphi^{-1}(\varphi(\pi(\mathcal{I}))) = \pi(\mathcal{I})$.

Theorem B.1 (Weak identifiability conditions). *For $E \in F(m,k)$, let $ran(E)_s = \{x \in ran\, E : x$ is s-sparse when expanded in $E.\}$. Let $s_1, s_2 \in \mathbb{N}_+$ be such that $s_1 + s_2 \leq m$ and let $k, l \in \mathbb{N}$ be such that $s_1 \leq k \leq m$, $s_2 \leq l \leq m$. Then, for Lebesgue almost all pairs $(E, D) \in F(m,k) \times F(m,l)$, the pair of vectors $(v, w) \in ran(E)_{s_1} \times ran(D)_{s_2}$ is identifiable up to scaling with respect to the circular convolution map $C : \mathbb{C}^m \times \mathbb{C}^m \to \mathbb{C}^m$, $(v, w) \mapsto v \circledast w$.*

Proof. The proof of this theorem can be given along the lines of the proof of Theorem III.5 respectively Proposition IV.4. The only difference is that the set $\mathcal{W}$ in Proposition IV.4 has to be replaced by the set $(vw^t - M^1_{s_1,s_2}(n_1,n_2)) \setminus \{0\}$. Clearly $vw^t - M^1_{s_1,s_2}(n_1,n_2)$ is isomorphic to $M^1_{s_1,s_2}(n_1,n_2)$ and thus $\dim(vw^t - M^1_{s_1,s_2}(n_1,n_2)) = \dim M^1_{s_1,s_2}(n_1,n_2) = s_1 + s_2 - 1$ by the proof of Proposition IV.1. □

The following theorem shows that this bound is indeed optimal.

Theorem B.2. *If a bilinear map $B \in \mathcal{B}(m)$ is such that $(u, v) \in \mathbb{C}^{n_1}_{s_1} \setminus \{0\} \times \mathbb{C}^{n_2}_{s_1} \setminus \{0\}$ is weakly identifiable up to scaling with respect to B then $m \geq s_1 + s_2$.*

Let us first give two propositions that allow us to prove this theorem.

Proposition B.3. *If there exists a bilinear map $B \in \mathcal{B}(m)$ such that $(v, w) \in \mathbb{C}^{n_1}_{s_1} \setminus \{0\} \times \mathbb{C}^{n_2}_{s_1} \setminus \{0\}$ is weakly identifiable up to scaling then there exists a linear map $M : M(s_1, s_2) \to \mathbb{C}^m$ such that $P(e_1 e_1^t - M^1(s_1, s_2)) \cap P(ker\, M) = \emptyset$* [9].

Proof. We stick to the notation introduced in Subsection IV B. Let $(v, w) \in \mathbb{C}^{n_1}_{s_1} \setminus \{0\} \times \mathbb{C}^{n_2}_{s_1} \setminus \{0\}$ and let $M_B : M(n_1, n_2) \to \mathbb{C}^m$ be the linear map induced by B. Clearly there exist $A \in \mathcal{A}(n_1, s_1)$, $B \in \mathcal{A}(n_2, s_2)$ such that $vw^t \in W_{A,B}$. Consider the isomorphism $\eta|_{M^1(s_1,s_2)} : M^1(s_1, s_2) \to W_{A,B}$ defined in (2). Let $U_1, U_2 \in M(s_1, s_2)$ be unitaries such that $\eta(U_1 e_1 e_1^t U_2) = vw^t$. Define a linear map $M : M(s_1, s_2) \to \mathbb{C}^m$ by setting $M(X) = M_B \circ \eta(U_1 X U_2)$ for all $X \in M(n_1, n_2)$. Now, assume for a contradiction that there is an $X = e_1 e_1^t - \tilde{v}\tilde{w}^t$ for some $\tilde{v} \in \mathbb{C}^{s_1} \setminus \{0\}$, $\tilde{w} \in \mathbb{C}^{s_2} \setminus \{0\}$ with $P(X) \in P(e_1 e_1^t - M^1(s_1, s_2)) \cap P(\ker M)$. Then we have $B(v, w) - B(I_A U_1 \tilde{v}, I_B U_2 \tilde{w}) = M_B(vw^t - \eta(U_1 \tilde{v}\tilde{w}^t U_2)) = M(X) = 0$, the sought contradiction. □

Proposition B.4. *The set $P^{-1}\left(P(e_1 e_1^t - M^1(s_1, s_2))\right)$ is the common zero locus of a set of homogeneous polynomials and $\dim P(e_1 e_1^t - M^1(s_1, s_2)) = s_1 + s_2 - 1$.*

Proof. For $1 \leq i < i' \leq s_1$ and $1 \leq j < j' \leq s_2$ define the 2×2 minors

$$M_{ij,i'j'} : M(s_1, s_2) \to \mathbb{C},\ X \mapsto \det \begin{pmatrix} X_{ij} & X_{ij'} \\ X_{i'j} & X_{i'j'} \end{pmatrix}.$$

Then $V_G = P^{-1}(P(e_1 e_1^t - M^1(s_1, s_2)))$ is the common zero locus of the set of homogeneous polynomials $G := \{M_{ij,i'j'}\}_{1 \leq i < i' \leq s_1, 1 \leq j < j' \leq s_2, (i,j) \neq (1,1)}$. To determine the dimension of $P(e_1 e_1^t - M^1(s_1, s_2))$ consider the injective morphism

$$\eta : \mathbb{C} \times (M^1(s_1, s_2) \cap \{X \in M(s_1, s_2) : X_{22} \neq 0\}) \to V_G,\ (\lambda, X) \to \lambda e_1 e_1^* + X.$$

[9] Here e_1 denotes the first basis vector of the standard orthonormal basis of $\mathbb{C}^n$.

Now note that $\dim(M^1(s_1,s_2)\cap\{X\in M(s_1,s_2): X_{22}\neq 0\}) = \dim M^1(s_1,s_2) = s_1+s_2-1$ [10] and hence we find $\dim P(e_1e_1^t - M^1(s_1,s_2)) = \dim\mathbb{C}+\dim M^1(s_1,s_2)-1 = s_1+s_2-1$. □

Now we are in a position to proof Theorem B.2.

Proof of Theorem B.2. Using Proposition B.3 it suffices to show that if for a linear map $M: M(s_1,s_2)\to\mathbb{C}^m$ one has $P(\ker M)\cap P(e_1e_1^t - M^1(s_1,s_2)) = \emptyset$, then $m\geq s_1+s_2$.

Clearly, for such an $M\in\mathcal{L}(m)$, $P(\ker M)$ is a projective algebraic set and, by Proposition B.4, $P(e_1e_1^t - M^1(s_1,s_2))$ is also a projective algebraic set. Then, the result follows again from the intersection theorem for projective varieties (cf. proof of Theorem III.1). □

[10] $M^1(s_1,s_2)$ is irreducible by Example 12.1 of [33] and hence $M^1(s_1,s_2)\cap\{X\in M(s_1,s_2): X_{22}\neq 0\}$ is irreducible as a non-empty open subset of the irreducible set $M^1(s_1,s_2)$ (see Exercise 1.1.3 of [32]). Finally we have $\dim(M^1(s_1,s_2)\cap\{X\in M(s_1,s_2): X_{22}\neq 0\}) = \dim M^1(s_1,s_2)$ by Exercise 1.6 and Proposition 1.10 of [32].

Stable Pure State Quantum Tomography from Five Orthonormal Bases

C. Carmeli, T. Heinosaari, M. Kech, J. Schultz and A. Toigo August 24, 2016

In [1], a measurement scheme consisting of four von Neumann measurements that allows the discrimination of any two pure quantum states is constructed. Starting from the construction of [1], this article provides a measurements scheme consisting of five von Neumann measurement which satisfies the following separation property (see [2, 3]).

Definition 1. (Pure state complete among all states.) A measurement scheme $M \in MS_{\mathbb{C}^n}$ is called pure state complete among all states (PCA) iff $D_M(\sigma) \neq D_M(\varrho)$ holds for all $\sigma \in \mathcal{S}_1(\mathbb{C}^n)$ and $\varrho \in \mathcal{S}(\mathbb{C}^n)$ with $\sigma \neq \varrho$.

If a measurement scheme $M \in MS_{\mathbb{C}^n}$ is PCA one can decide from the outcome distributions $D_M(\varrho)$ whether or not a quantum $\varrho \in \mathcal{S}(\mathbb{C}^n)$ is pure. However, most notably PCA measurement schemes allow for a computationally tractable tomography of pure quantum states.

1 Main Result

Denote by $e_0, \ldots, e_{n-1}$ the standard orthonormal basis of $\mathbb{C}^n$ and set $v_j^0 := e_j$, for $j = 0, \ldots, d-1$. For $j = 0, \ldots, d-1$, let

$$v_j^1 := \sqrt{\frac{2}{d+1}} \left(\sin\left(1\,\frac{j+1}{d+1}\,\pi\right), \sin\left(2\,\frac{j+1}{d+1}\,\pi\right), \ldots, \sin\left(d\,\frac{j+1}{d+1}\,\pi\right)\right),$$

$$v_j^2 := \sqrt{\frac{2}{d+1}} \left(\sin\left(1\,\frac{j+1}{d+1}\,\pi\right), \sin\left(2\,\frac{j+1}{d+1}\,\pi\right) e^{i\pi/d}, \ldots, \sin\left(d\,\frac{j+1}{d+1}\,\pi\right) e^{i(d-1)\pi/d}\right).$$

Similarly, for $j = 0, \ldots, d-2$, let

$$v_j^3 := \sqrt{\frac{2}{d}} \left(\sin\left(1\,\frac{j+1}{d}\,\pi\right), \sin\left(2\,\frac{j+1}{d}\,\pi\right), \ldots, \sin\left((d-1)\frac{j+1}{d}\,\pi\right), 0\right),$$

$$v_j^4 := \sqrt{\frac{2}{d}} \left(\sin\left(1\,\frac{j+1}{d}\,\pi\right), \sin\left(1\,\frac{j+1}{d}\,\pi\right) e^{i\pi/d}, \ldots, \sin\left((d-1)\frac{j+1}{d}\,\pi\right) e^{i(d-2)\pi/d}, 0\right)$$

and set $v_{d-1}^3 := e_{n-1}$ as well as $v_{d-1}^4 := e_{n-1}$.

Theorem 1. *The multisets* $P^i := \{v_j^i (v_j^i)^* \,|\, j \in \{0, \ldots, d-1\}\}$, $i = 0, 1, 2, 3, 4$, *are von Neumann measurements and the measurement scheme* $M := (P_0, P_1, P_2, P_3, P_4)$ *is PCA.*

2 Stability

Let $\sigma \in \mathcal{S}_1(\mathbb{C}^n)$ be a pure state, let $f \in \mathbb{R}^{5n}$ be an error term and let $M \in MS_{\mathcal{H}}$ be a PCA measurement scheme. Consider the convex program

$$\begin{aligned} &\text{minimize } \|D_M(Y) - b\| \\ &\text{subject to } Y \geq 0, \end{aligned} \tag{1}$$

where $b := D_M(\sigma) + f$ is the noisy measurement outcome.

Then, the following qualitative recovery result holds.

Theorem 2 (Stable Recovery)**.** *Let $\epsilon > 0$. There is a constant $C_M > 0$ independent of ϵ such that for all pure states σ and all error terms $f \in \mathbb{R}^{5n}$ with $\|f\| \leq \epsilon$, any minimizer Y^* of* (1) *satisfies*

$$\|Y^* - \sigma\|_{HS} \leq C_M \epsilon.$$

3 Legal statement

I am the principal author of this article and I was significantly involved in all parts of this article.

References

[1] Philippe Jaming. Uniqueness results in an extension of pauli's phase retrieval problem. *Applied and Computational Harmonic Analysis*, 37(3):413–441, 2014.

[2] Jianxin Chen, Hillary Dawkins, Zhengfeng Ji, Nathaniel Johnston, David Kribs, Frederic Shultz, and Bei Zeng. Uniqueness of quantum states compatible with given measurement results. *Physical Review A*, 88(1):012109, 2013.

[3] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. Tasks and premises in quantum state determination. *Journal of Physics A: Mathematical and Theoretical*, 47(7):075302, 2014.

Stable Pure State Quantum Tomography from Five Orthonormal Bases

Claudio Carmeli[1], Teiko Heinosaari[2], Michael Kech[3], Jussi Schultz[2] and Alessandro Toigo[4,5]

[1] *DIME, Università di Genova - Via Magliotto 2, I-17100 Savona, Italy*
[2] *Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku - FI-20014 Turku, Finland*
[3] *Department of Mathematics, Technische Universität München - 85748 Garching, Germany*
[4] *Dipartimento di Matematica, Politecnico di Milano - Piazza Leonardo da Vinci 32, I-20133 Milano, Italy*
[5] *I.N.F.N., Sezione di Milano - Via Celoria 16, I-20133 Milano, Italy*

PACS 03.65.Wj – State reconstruction, quantum tomography
PACS 03.65.Aa – Quantum systems with finite Hilbert space
PACS 03.65.Ta – Foundations of quantum mechanics; measurement theory

Abstract – For any finite dimensional Hilbert space, we construct explicitly five orthonormal bases such that the corresponding measurements allow for efficient tomography of an arbitrary pure quantum state. This means that such measurements can be used to distinguish an arbitrary pure state from any other state, pure or mixed, and the pure state can be reconstructed from the outcome distribution in a feasible way. The set of measurements we construct is independent of the unknown state, and therefore our results provide a fixed scheme for pure state tomography, as opposed to the adaptive (state dependent) scheme proposed by Goyeneche *et al.* in [*Phys. Rev. Lett.* **115**, 090401 (2015)]. We show that our scheme is robust with respect to noise, in the sense that any measurement scheme which approximates these measurements well enough is equally suitable for pure state tomography. Finally, we present two convex programs which can be used to reconstruct the unknown pure state from the measurement outcome distributions.

Introduction. – The aim of quantum tomography is to reconstruct the unknown state of a quantum system by performing suitable measurements on it. Tomography is a vital routine in quantum information, where it is used to characterize output states and test processing devices. However, quantum tomography is a consuming task: in order to obtain enough information for state reconstruction of a d-level system, it is necessary to perform measurements of $d+1$ different orthonormal bases, or a generalized measurement with at least d^2 outcomes. This poor scaling has led to the search for more efficient methods which allow for a reduction of resources in specific cases.

Recent focus has been on the identification of unknown pure (or more generally low rank) states [1–7]. Any two pure states can be distinguished with a measurement having just $\sim 4d$ outcomes [1] or, when restricting to projective measurements, with only four orthonormal bases [3, 7, 8]. The drawback of these approaches is that the measurements they provide cannot distinguish pure states from *all* states, implying that one needs to know that the state is pure prior to the measurement in order not to confuse it with mixed states having the same measurement outcome distributions. Moreover, none of the approaches allows an efficient recovery algorithm, mainly since the non-convex nature of the problem renders usual techniques from convex optimization useless.

In [9], a scheme involving five orthonormal bases along with a reconstruction algorithm was proposed and experimentally demonstrated. Remarkably, such a scheme allows to certify the purity assumption on the state directly from the measurement outcomes. However, this method is adaptive in the sense that the outcome distribution of the first measurement affects the choice of the subsequent ones. Therefore, if one requires the procedure to work for all pure states the overall number of required measurement settings is considerably larger than five.

At the cost of a slightly higher number $\mathcal{O}(d \ln d)$ of measurement outcomes, tomographic procedures based on compressed sensing were proposed in [10–12]. This approach allows for the stable recovery of pure quantum

states, as well as satisfies the requirement of distinguishing pure states from all states [13]. However, rather than providing a functioning measurement set-up, compressed sensing techniques guarantee that, with high probability, any state can be reconstructed by using sufficiently many randomly drawn measurement settings. From a practical point of view, however, a deterministic approach which provides an explicit measurement set-up may be favourable.

In this Letter we overcome these drawbacks by constructing five orthonormal bases such that every pure state can be efficiently reconstructed from the corresponding measurements. For any dimension d, our set of measurements is fixed and therefore there is no need for data processing in between the measurements. We show that these measurements distinguish pure states from all states, and this therefore shows that the scaling $\sim 5d$ in the total number of outcomes is the same as without the constraint of having projective measurements [14]. More importantly, we prove that the presented set-up is robust with respect to noise. Finally, we provide reconstruction algorithms for the practical retrieval of the unknown state from the measurement data. We remark that, as compared to the compressed sensing results of [10–12], our result comes with fewer measurement outcomes. However, the stability guarantees that we can derive are weaker.

Construction of the bases. – We begin by constructing, for any dimension d, five orthonormal bases $\mathcal{B}^0, \dots, \mathcal{B}^4$ which determine any pure state among all states. This means that for any pure state represented by a unit vector ψ, and any density matrix ϱ, the equalities

$$\left|\langle v_j^\ell \mid \psi\rangle\right|^2 = \langle v_j^\ell \mid \varrho\, v_j^\ell\rangle \quad \text{for all } v_j^\ell \in \mathcal{B}^\ell \text{ and } \ell = 0, \dots, 4$$

imply that $\varrho = |\psi\rangle\langle\psi|$. The construction is an extension of [8] where, based on the properties of Hermite polynomials, four orthonormal bases $\mathcal{B}^1, \dots, \mathcal{B}^4$ capable of distinguishing any two pure states were presented. That construction generalizes easily to any sequence of orthogonal polynomials as explained in [3]. Remarkably, by adding the canonical basis $\mathcal{B}^0 = \{e_0, \dots, e_{d-1}\}$ to this set, we obtain the five bases with the desired property.

To begin with, let us fix a *sequence of orthogonal polynomials*, that is, a sequence $(p_n)_{n=0}^\infty$ of real polynomials such that p_n is of degree n and

$$\langle p_j, p_i\rangle := \int_{-\infty}^{\infty} p_j(x)p_i(x)w(x)dx = \delta_{ij}$$

for some positive weight function w. For a d-dimensional system we will only need the first $d+1$ polynomials. To construct the first two bases, let $x_0, \dots, x_{d-1}$ be the zeros of p_d, which are real and distinct numbers satisfying $p_{d-1}(x_j) \neq 0$ for all $j \in \{0, \dots, d-1\}$ [15, Section 3.3]. Pick an $\alpha \in \mathbb{R}$ such that $e^{ij\alpha} \notin \mathbb{R}$ for all $j \in \{1, \dots, d-1\}$. Now for $j = 0, \dots, d-1$, set

$$v_j^1 := (p_0(x_j), p_1(x_j), \dots, p_{d-1}(x_j))\,,$$
$$v_j^2 := \left(p_0(x_j), e^{i\alpha}p_1(x_j), \dots, e^{i(d-1)\alpha}p_{d-1}(x_j)\right)$$

and denote $\mathcal{B}^1 = \{v_j^1/\|v_j^1\| \mid j = 0, \dots, d-1\}$ and $\mathcal{B}^2 = \{v_j^2/\|v_j^2\| \mid j = 0, \dots, d-1\}$. The fact that these are actually orthonormal bases can be readily checked using the Christoffel-Darboux formula [15, Theorem 3.2.2]

$$\sum_{i=0}^{n} p_i(x)p_i(y) = \frac{k_n}{k_{n+1}} \frac{p_{n+1}(x)p_n(y) - p_n(x)p_{n+1}(y)}{x-y}$$

where k_n is the leading coefficient of p_n (see [3,8] for more details). This formula evaluated at $n = d-1$ and $x = y = x_j$ also yields the normalization factor

$$\left\|v_j^1\right\|^2 = \left\|v_j^2\right\|^2 = \frac{k_{d-1}}{k_d}\, p_d'(x_j)p_{d-1}(x_j).$$

For the remaining two bases, let $y_0, \dots, y_{d-2}$ be the zeros of p_{d-1}. As the polynomials p_d and p_{d-1} have no common zeros, the y_j:s are distinct from the x_j:s. By a similar reason, $p_{d-2}(y_j) \neq 0$ for all $j = 0, \dots, d-2$. For $j = 0, \dots, d-2$ define the non-zero vectors

$$v_j^3 := (p_0(y_j), p_1(y_j), \dots, p_{d-2}(y_j), 0)\,,$$
$$v_j^4 := \left(p_0(y_j), e^{i\alpha}p_1(y_j), \dots, e^{i(d-2)\alpha}p_{d-2}(y_j), 0\right)\,,$$

and by setting $v_{d-1}^3 := e_{d-1}$ as well as $v_{d-1}^4 := e_{d-1}$ we have arrived at the two orthonormal bases $\mathcal{B}^3 = \{v_j^3/\|v_j^3\| \mid j = 0, \dots, d-1\}$ and $\mathcal{B}^4 = \{v_j^4/\|v_j^4\| \mid j = 0, \dots, d-1\}$. The normalization is now given by

$$\left\|v_j^3\right\|^2 = \left\|v_j^4\right\|^2 = \frac{k_{d-2}}{k_{d-1}}\, p_{d-1}'(y_j)p_{d-2}(y_j).$$

Theorem 1. *The five orthonormal bases $\mathcal{B}^0, \dots, \mathcal{B}^4$ constructed above determine any pure state among all states.*

Proof. Let $\psi = \sum_{j=0}^{d-1} c_j e_j$ be a unit vector and let ϱ be an arbitrary state such that $\left|\langle v_j^\ell \mid \psi\rangle\right|^2 = \langle v_j^\ell \mid \varrho\, v_j^\ell\rangle$ for all $v_j^\ell \in \mathcal{B}^\ell$ and $\ell = 0, \dots, 4$. From the standard basis $\mathcal{B}^0$ we get $\varrho_{k,k} = |c_k|^2$ for all k. Let n denote the largest number such that $\varrho_{n,n} = |c_n|^2 \neq 0$ so that by the positivity of ϱ, $\varrho_{k,l} = \varrho_{l,k} = 0$ for all $k > n$. By the definition of the bases and the equalities of the probabilities we then have

$$\sum_{k,l=0}^{n} (\varrho_{k,l} - c_k\bar{c}_l)p_k(z)p_l(z) = 0 \tag{1}$$

$$\sum_{k,l=0}^{n} (\varrho_{k,l} - c_k\bar{c}_l)e^{i(l-k)\alpha}p_k(z)p_l(z) = 0 \tag{2}$$

for all $z = x_j$ and $z = y_j$, but since the polynomials have degree at most $2n \leq 2d-2$ and they vanish on $2d-1$ distinct points, they must be identically zero. In other

words, the above equalities must hold for all $z \in \mathbb{R}$. Let us denote $t_{k,l} = \varrho_{k,l} - c_k\overline{c}_l$ so that $t_{l,k} = \overline{t_{k,l}}$ and $t_{k,k} = 0$. By looking at the highest degree terms in (1) and (2) we get $\mathrm{Re}\,(t_{n,n-1}) = \mathrm{Re}\,(e^{-i\alpha}t_{n,n-1}) = 0$, which imply that $t_{n,n-1} = 0$. In other words, the matrix elements of the two states coincide on the diagonal and the bottom right $(d-n+1)\times(d-n+1)$-block. We now proceed by induction.

Firstly, whenever the two states coincide on some bottom right $(d-r)\times(d-r)$-block, with $1 \le r \le n-1$, we have $t_{k,l} = 0$ for $k \ge r$ and $l \ge r$. But then the highest degree terms in (1) and (2) give $\mathrm{Re}\,(t_{n,r-1}) = \mathrm{Re}\,(e^{i(r-n-1)\alpha}t_{n,r-1}) = 0$, which yield $t_{n,r-1} = 0$, that is $\varrho_{n,r-1} = c_n\overline{c_{r-1}}$. Secondly, using this and the positivity of ϱ we can calculate for all $r-1 < k < n$

$$\begin{aligned} 0 \le & \begin{vmatrix} \varrho_{r-1,r-1} & \varrho_{r-1,k} & \varrho_{r-1,n} \\ \varrho_{k,r-1} & \varrho_{k,k} & \varrho_{k,n} \\ \varrho_{n,r-1} & \varrho_{n,k} & \varrho_{n,n} \end{vmatrix} \\ = & \begin{vmatrix} |c_{r-1}|^2 & \varrho_{r-1,k} & c_{r-1}\overline{c_n} \\ \overline{\varrho_{r-1,k}} & |c_k|^2 & c_k\overline{c_n} \\ \overline{c_{r-1}}c_n & \overline{c_k}c_n & |c_n|^2 \end{vmatrix} \\ = & -|c_n|^2|\varrho_{r-1,k} - c_{r-1}\overline{c_k}|^2 \end{aligned}$$

which is satisfied if and only if the right-hand side is zero. Since $c_n \neq 0$, this gives us $\varrho_{r-1,k} = c_{r-1}\overline{c_k}$. The two states therefore coincide on a larger bottom right block. By induction, the states must be equal. □

To give an example of the previously explained construction of five bases, we take the Chebyshev polynomials of the second kind $(U_n)_{n=0}^{\infty}$. These are the unique polynomials such that [15, p. 3]

$$U_n(\cos\theta) = \frac{\sin\left((n+1)\theta\right)}{\sin\theta}$$

holds for all $n = 0, 1, \ldots$ and $\theta \in [0, 2\pi)$. The n roots of U_n are given by

$$\cos\left(\frac{j+1}{n+1}\,\pi\right),\ j = 0, \ldots, n-1\,,$$

and its leading coefficient is $k_n = 2^n$. Hence, the normalized vectors of the first and the third basis are

$$v_j^1 = \sqrt{\frac{2}{d+1}}\left(\sin\left(1\,\frac{j+1}{d+1}\,\pi\right), \ldots, \sin\left(d\,\frac{j+1}{d+1}\,\pi\right)\right)$$

$$v_j^3 = \sqrt{\frac{2}{d}}\left(\sin\left(1\,\frac{j+1}{d}\,\pi\right), \ldots, \sin\left((d-1)\frac{j+1}{d}\,\pi\right), 0\right)$$

with $v_{d-1}^3 = (0, \ldots, 0, 1)$. The bases $\mathcal{B}^2$ and $\mathcal{B}^4$ are similar.

More general measurements and stability. – A realistic measurement is affected by noise and therefore cannot be described simply by an orthonormal basis. Even more, an optimal measurement for a given task might not even be related to an orthonormal basis. For these reasons, one needs to have a wider mathematical framework for measurements. A general measurement in quantum mechanics can be modelled by a positive operator valued measure (POVM) [16], which is a function $j \mapsto P(j)$ from a finite set of measurement outcomes $\{1, \ldots, m\}$ to the linear space of $d \times d$ Hermitian matrices $H(d)$ such that $P(j) \ge 0$ and $\sum_{j=1}^{m} P(j) = \mathbb{1}$. In practice one might want to measure more than one POVM. For instance, a noisy measurement of each orthonormal basis can be described by a separate POVM. By a *measurement scheme* we mean a set $\mathcal{Q} := \{P_1, \ldots, P_l\}$ of POVMs. It is not restrictive to assume that all POVMs in a given measurement scheme have the same set of outcomes $\{1, \ldots, m\}$. A measurement scheme $\mathcal{Q}$ therefore induces a linear map $M_{\mathcal{Q}}$ from the real vector space $H(d)$ to the set of real $l \times m$ matrices $M_{lm}(\mathbb{R})$ via

$$M_{\mathcal{Q}}(X)_{i,j} = \mathrm{tr}\,[XP_i(j)]\,.$$

The image of a state ϱ is the real matrix whose i-th row contains the outcome probabilities corresponding to P_i. Analogously to the case of projective measurements, we say that the measurement scheme $\mathcal{Q}$ determines any pure state among all states if for any pure state $\sigma = |\psi\rangle\langle\psi|$ and any state ϱ, the equality $M_{\mathcal{Q}}(\sigma) = M_{\mathcal{Q}}(\varrho)$ implies $\varrho = \sigma$. By adapting the argument of [2, Theorem 1], we obtain the following characterization.

Proposition 1. *A measurement scheme $\mathcal{Q}$ determines any pure state among all states if and only if every non-zero element of* $\ker M_{\mathcal{Q}}$ *has at least two positive eigenvalues.*

Proof. The measurement scheme $\mathcal{Q}$ does not determine pure states among all states if and only if $M_{\mathcal{Q}}(\sigma - \varrho) = 0$ for some states σ and ϱ such that σ is pure and $\sigma - \varrho \neq 0$. This implies that $\sigma - \varrho \in \ker M_{\mathcal{Q}}$, and $\sigma - \varrho$ has at most one positive eigenvalue by Weyl's inequalities [17, Theorem III.2.1]. Conversely, if $X \in \ker M_{\mathcal{Q}}$ is non-zero and has at most one positive eigenvalue, then it has exactly one positive eigenvalue since $\mathrm{tr}\,[X] = \sum_j M_{\mathcal{Q}}(X)_{i,j} = 0$. Hence, its positive part X_+ has rank 1. Defining the states $\sigma = X_+/\mathrm{tr}\,[X_+]$ and $\varrho = (X_+ - X)/\mathrm{tr}\,[X_+]$, we have that σ is pure, $\sigma - \varrho = X/\mathrm{tr}\,[X_+] \neq 0$ and $M_{\mathcal{Q}}(\sigma - \varrho) = M_{\mathcal{Q}}(X)/\mathrm{tr}\,[X_+] = 0$. □

With this framework of measurement schemes we are now prepared to discuss the noise robustness of the result stated in Theorem 1. First, we will need to have a notion of closeness of two measurement schemes, and for this reason we fix norms on the real vector spaces $H(d)$ and $M_{lm}(\mathbb{R})$. Since these are finite dimensional vector spaces, all norms are equivalent and the choice is not important for our purposes. Typical choices are, e.g., the trace norm $\|X\| = \mathrm{tr}\,[|X|]$ on $H(d)$, and on $M_{lm}(\mathbb{R})$ the supremum of the ℓ^1-norm over all lines, i.e.,

$$\|M\| = \sup_i \sum_j |M_{i,j}|\,.$$

The inequality $\|M_{\mathcal{Q}}(\varrho) - M_{\mathcal{Q}'}(\varrho)\| \leq \epsilon$ then means that the measurement outcome distributions of all the POVMs in $\mathcal{Q}$ and $\mathcal{Q}'$ measured on the same state ϱ are uniformly close in the total variation norm. We will say that two measurement schemes $\mathcal{Q}$ and $\mathcal{Q}'$ are *ϵ-close* if $\|M_{\mathcal{Q}} - M_{\mathcal{Q}'}\|_\infty < \epsilon$, where $\|\cdot\|_\infty$ is the uniform operator norm in the chosen norms of $H(d)$ and $M_{lm}(\mathbb{R})$.

Theorem 2 (Stability)**.** *If a measurement scheme $\mathcal{Q}$ determines any pure state among all states, then there is an $\epsilon > 0$ such that every measurement scheme $\mathcal{Q}'$ which is ϵ-close to $\mathcal{Q}$ has this same property.*

Proof. For $i \in \{1, \ldots, d\}$, denote by $\lambda_i(X)$ the i-th greatest eigenvalue of a Hermitian matrix $X \in H(d)$. Let $K := \{X \in H(d) : \lambda_2(X) \leq 0, \|X\| = 1\}$ be the set of unit norm Hermitian matrices with at most one positive eigenvalue. Consider the map $\phi : H(d) \to \mathbb{R}^d$,

$$\phi(X) = (\lambda_1(X), -\lambda_2(X), \ldots, -\lambda_d(X))$$

and let $L := [0, +\infty)^d$. We have $K = \phi^{-1}(L) \cap H(d)_1$, where $H(d)_1$ is the unit sphere in $H(d)$. Since $H(d)_1$ is compact, L is closed, and ϕ is continuous by Weyl's perturbation theorem [17, Corollary III.2.6], we conclude that K is a compact set.

We claim that a measurement scheme $\mathcal{Q}$ determines pure states among all states if and only if $c := \min_{X \in K} \|M_{\mathcal{Q}}(X)\| > 0$. First, assume $c > 0$, and let $X \neq 0$ be such that $\lambda_2(X) \leq 0$. We have $X/\|X\| \in K$, hence

$$\|M_{\mathcal{Q}}(X)\| = \|X\| \left\| M_{\mathcal{Q}}\left(\frac{X}{\|X\|}\right)\right\| \geq c\,\|X\| \neq 0,$$

that is, $X \notin \ker M_{\mathcal{Q}}$. Therefore, $\mathcal{Q}$ determines any pure state among all states by Proposition 1. Conversely, suppose that $\mathcal{Q}$ has the latter property. By the compactness of K, there is $X \in K$ such that $c = \|M_{\mathcal{Q}}(X)\|$. Since Proposition 1 implies that every non-zero element of $\ker M_{\mathcal{Q}}$ has at least two positive eigenvalues, we have $M_{\mathcal{Q}}(X) \neq 0$ and thus $c \neq 0$.

Finally, if $\|M_{\mathcal{Q}} - M_{\mathcal{Q}'}\|_\infty < \epsilon$, then

$$\min_{X \in K} \|M_{\mathcal{Q}'}(X)\| \geq \min_{X \in K} (\|(M_{\mathcal{Q}}(X)\| - \|(M_{\mathcal{Q}} - M_{\mathcal{Q}'})(X)\|) \geq c - \epsilon.$$

Hence, for any $\epsilon < c$, the measurement scheme $\mathcal{Q}'$ determines any pure state among all states. □

Pure state quantum tomography. – The most notable practical feature of measurement schemes that determine pure states among all states is that they allow for a computationally efficient tomography of pure quantum states. Essentially, this is due to the fact that for every pure state σ, the unique solution to the feasibility problem

$$\begin{aligned} &\text{find } X \\ &\text{subject to } X \geq 0,\ M_{\mathcal{Q}}(X) = M_{\mathcal{Q}}(\sigma) \end{aligned}$$

is given by σ. Indeed, since $\operatorname{tr}[X] = \sum_j M_{\mathcal{Q}}(X)_{i,j}$, the constraints imply that any solution is a state. Such a state must then coincide with σ, as the measurement scheme $\mathcal{Q}$ determines σ among all states.

In practice, the state σ might not be pure, but just well approximated by a pure state, the measurement $M_{\mathcal{Q}}(\sigma)$ might be affected by systematic errors and furthermore there is statistical noise. Because of that, in a realistic scenario, one has to reconstruct σ from the perturbed measurement data $b := M_{\mathcal{Q}}(\sigma) + f$, where $f \in M_{lm}(\mathbb{R})$ is a small error term capturing all of these sources of error. In the remainder of this section we present two convex optimization problems which allow for a recovery of any pure state σ from the noisy measurement data b provided that the measurement scheme $\mathcal{Q}$ determines pure states among all states. Results in this direction have been reported also in [18].

First, consider the well-known [19] semi-definite program

$$\begin{aligned} &\text{minimize } \operatorname{tr}(Y) \\ &\text{subject to } Y \geq 0,\ \|M_{\mathcal{Q}}(Y) - b\| \leq \epsilon, \end{aligned} \tag{3}$$

where $\epsilon > 0$ is an error scale which has to be fixed in advance. Then, as an easy consequence of [20, Theorem IV.1], we get the following recovery result (a simple proof is reported below).

Theorem 3 (Stable Recovery I)**.** *Let $\epsilon > 0$. There is a constant $C_{\mathcal{Q}} > 0$ independent of ϵ such that for all pure states σ and all error terms $f \in M_{lm}(\mathbb{R})$ with $\|f\| \leq \epsilon$, any minimizer Y^* of* (3) *satisfies*

$$\|Y^* - \sigma\| \leq C_{\mathcal{Q}}\epsilon.$$

Secondly, consider the following convex program, which was also proposed in [21]

$$\begin{aligned} &\text{minimize } \|M_{\mathcal{Q}}(Y) - b\|_2 \\ &\text{subject to } Y \geq 0. \end{aligned} \tag{4}$$

Note that, different from the program (3), there is no need to guess an error scale ϵ in advance, which might be desirable from a practical point of view. The next result then follows from [20, Lemma V.5] (see also below).

Theorem 4 (Stable Recovery II)**.** *Let $\epsilon > 0$. There is a constant $C_{\mathcal{Q}} > 0$ independent of ϵ such that for all pure states σ and all error terms $f \in M_{lm}(\mathbb{R})$ with $\|f\| \leq \epsilon$, any minimizer Y^* of* (4) *satisfies*

$$\|Y^* - \sigma\| \leq C_{\mathcal{Q}}\epsilon.$$

Proof of Theorems 3 and 4. Note that for both of the optimizations (3) and (4) the minimizer Y^* satisfies $\|M_{\mathcal{Q}}(Y^*) - M_{\mathcal{Q}}(\sigma) - f\| \leq \epsilon$. Hence, in both cases we find

$$\begin{aligned} \epsilon &\geq \|M_{\mathcal{Q}}(Y^*) - M_{\mathcal{Q}}(\sigma) - f\| \geq \|M_{\mathcal{Q}}(Y^* - \sigma)\| - \|f\| \\ &\geq \|Y^* - \sigma\| \inf_{\substack{X, \sigma' \geq 0,\ X \neq \sigma' \\ \operatorname{rank} \sigma' = 1}} \frac{\|M_{\mathcal{Q}}(\sigma' - X)\|}{\|\sigma' - X\|} - \epsilon. \end{aligned} \tag{5}$$

By Weyl's inequalities,

$$\left\{ \frac{\sigma' - X}{\|\sigma' - X\|} : \ X, \sigma' \geq 0, \ X \neq \sigma' \text{ and } \operatorname{rank} \sigma' = 1 \right\} \subseteq K \,,$$
$$\text{where} \quad K := \{X' \in H(d) : \lambda_2(X') \leq 0, \ \|X'\| = 1\} \,.$$

(Actually, it is easy to see that the two sets are equal.) By the argument in the proof of Theorem 2, the set K is compact. Since the measurement scheme $\mathcal{Q}$ determines pure states among all states, we have $M_{\mathcal{Q}}(X') \neq 0$ for all $X' \in K$ by Proposition 1, and hence

$$c_{\mathcal{Q}} := \min_{X' \in K} \|M_{\mathcal{Q}}(X')\| > 0.$$

This, together with (5), implies

$$\|Y^* - \sigma\|_2 \leq \frac{2}{c_{\mathcal{Q}}} \epsilon$$

and hence we can choose $C_{\mathcal{Q}} = 2/c_{\mathcal{Q}}$. □

Note that in both Theorems 3 and 4, the constant $C_{\mathcal{Q}}$ appearing in the stability bound might depend on all the parameters of $\mathcal{Q}$. We do not know how to estimate $C_{\mathcal{Q}}$ and hence we cannot make our stability results more explicit. Therefore, we have to rely on numerical simulations to evaluate whether the measurement schemes we constructed perform well enough in practise.

Numerical results. – For our simulations we choose the measurement schemes constructed from the Chebyshev polynomials of the second kind $(U_n)_{n=0}^{\infty}$. Moreover, we choose $\alpha = \pi/d$ and we use the Hilbert-Schmidt norm $\|\cdot\|_2$ on both $H(d)$ and $M_{lm}(\mathbb{R})$. For dimensions $d = 10, 20, \ldots, 60$, we ran the semi-definite program (3) for 10^5 times, where we sampled the pure states and error terms $f \in M_{lm}(\mathbb{R})$ with $\|f\|_2 = \epsilon$ independently according to the respective Haar measures. The error scale was set to $\epsilon = 10^{-4}$.

Figure 1 shows the empiric probability density function of the reconstruction error for the dimensions $d = 10, 30, 50$. In all cases the distribution appears to be well located, indicating a good reconstruction for most signals.

Figure 2 shows the empiric 96%,99% and 99.75% quantiles of the reconstruction error as well as its arithmetic mean. In the selected range of dimension the 99.75% quantile error does not exceed 60ϵ. This suggests that for most signals the reconstruction is feasible. Furthermore, all quantiles appear to scale sublinearly with the dimension.

Conclusion. – We have presented an explicit construction of five measurement settings which allow the efficient reconstruction of pure quantum states. Unlike earlier approaches, our method is deterministic and non-adaptive, meaning that the setting is fixed and works for all states. An important fact from the practical point of view is that the scheme is robust with respect to noise.

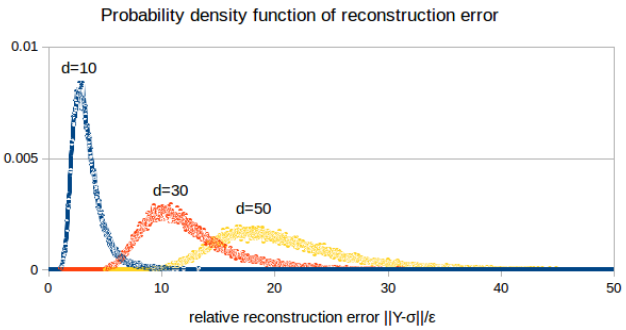

Fig. 1: (Color online) The empiric probability density function of the relative reconstruction error $\|Y^* - \sigma\|_2/\epsilon$ for dimensions $d = 10, 30, 50$, where Y^* is the minimizer of the semi-definite program (3).

Thus, state reconstruction from the measurement data can then be applied at the practical level by using the presented algorithms.

REFERENCES

[1] T. Heinosaari, L. Mazzarella, and M. M. Wolf. Quantum tomography under prior information. *Comm. Math. Phys.*, 318:355–374, 2013.

[2] C. Carmeli, T. Heinosaari, J. Schultz, and A. Toigo. Tasks and premises in quantum state determination. *J. Phys. A: Math. Theor.*, 47:075302, 2014.

[3] C. Carmeli, T. Heinosaari, J. Schultz, and A. Toigo. How many orthonormal bases are needed to distinguish all pure quantum states? *Eur. Phys. J. D*, 69:179, 2015.

[4] X. Ma, T. Jackson, H. Zhou, J. Chen, D. Lu, M. D. Mazurek, K. A. G. Fisher, X. Peng, D. Kribs, K. J. Resch, Z. Ji, B. Zeng, and R. Laflamme. Pure-state tomography with the expectation value of Pauli operators. *Phys. Rev. A*, 93:032140, 2016.

[5] M. Kech, P. Vrana, and M. M. Wolf. The role of topology in quantum tomography. *J. Phys. A: Math. Theor.*, 48:265303, 2015.

[6] M. Kech and M. M. Wolf. Quantum tomography of semi-algebraic sets with constrained measurements. *arXiv:1507.00903*, 2015.

[7] D. Mondragon and V. Voroninski. Determination of all pure quantum states from a minimal number of observables. *arXiv:1306.1214*, 2013.

[8] P. Jaming. Uniqueness results in an extension of Pauli's phase retrieval problem. *Appl. Comput. Harm. Anal.*, 37:413–441, 2014.

[9] D. Goyeneche, G. Cañas, S. Etcheverry, E. S. Gómez, G. B. Xavier, G. Lima, and A. Delgado. Five measurement bases determine pure quantum states on any dimension. *Phys. Rev. Lett.*, 115:090401, 2015.

[10] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.*, 105:150401, 2010.

[11] D. Gross. Recovering low-rank matrices from few coefficients in any basis. *IEEE Trans. Inf. Theory*, 57:1548–1566, 2011.

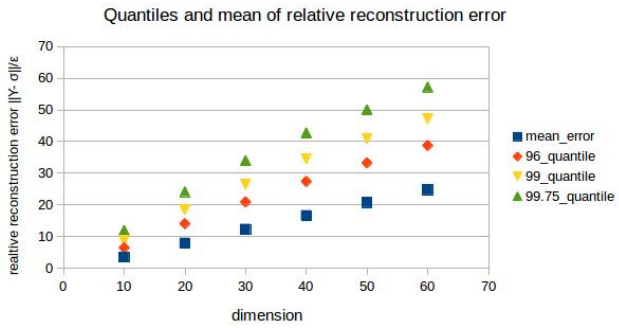

Fig. 2: (Color online) The empiric 96%, 99% and 99,75% quantiles as well as the mean of the relative reconstruction error $\|Y^* - \sigma\|_2/\epsilon$ for dimensions $d = 10, 20, \ldots, 60$, where Y^* is the minimizer of the semi-definite program (3).

[12] S. T. Steven, D. Gross, Y.-K. Liu, and J. Eisert. Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators. *New J. Phys.*, 14:095022, 2012.

[13] A. Kalev, R.L. Kosut, I.H. Deutsch. Quantum tomography protocols with positivity are compressed sensing protocols. *Npj Quantum Information* 1, 15018 (2015).

[14] J. Chen, H. Dawkins, Z. Ji, N. Johnston, D. Kribs, F. Shultz, and B. Zeng. Uniqueness of quantum states compatible with given measurement results. *Phys. Rev. A*, 88:012109, 2013.

[15] G. Szegö. *Orthogonal polynomials*. Fourth edition. American Mathematical Society, Colloquium Publications, Vol. XXIII. American Mathematical Society, Providence, R.I., 1975.

[16] T. Heinosaari and M. Ziman. *The mathematical language of quantum theory: From uncertainty to entanglement*. Cambridge University Press, Cambridge, 2012.

[17] R. Bhatia. *Matrix analysis*. Graduate Texts in Mathematics, Vol. 169. Springer-Verlag, New York, 1997.

[18] C. H. Baldwin, I. H. Deutsch and A. Kalev. Strictly-complete measurements for bounded-rank quantum-state tomography. *Phys. Rev. A*, 93:052105, 2016.

[19] B. Recht, M. Fazel, and P. A. Parrilo. Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization. *SIAM Rev.*, 52:471–501, 2010.

[20] M. Kech. Explicit frames for deterministic phase retrieval via phaselift. *arXiv:1508.00522*, 2015.

[21] M. Kabanava, R. Kueng, H. Rauhut, and U. Terstiege. Stable low-rank matrix recovery via null space properties. *arXiv:1507.07184*, 2015.

Subject: Re: Permission for EPL G37012/B18039
From: editorial.office@epletters.net
Date: 09.08.2016 10:11
To: kech@gmx.de

Dear Mr. Kech,

Many thanks for your message.
In answer to your request, we are pleased to inform you that you are allowed to use:

The article by

Claudio Carmeli, Teiko Heinosaari, Michael Kech, Jussi Schultz and Alessandro Toigo

"Stable pure state quantum tomography from five orthonormal bases"

You will have to wait until the references of the paper are available since the references of the source must be given (title, year, issue).
Thank you.

Sincerely yours,

Frederic Burr
EPL Staff Editor

Dear Sir or Madame,

I am currently preparing a cumulative dissertation. I am an author of the article

Stable pure state quantum tomography from five orthonormal bases
by Claudio Carmeli, Teiko Heinosaari, Michael Kech, Jussi Schultz and Alessandro Toigo

which was accepted for publication in EPL (reference number EPL G37012/B18039) and I would like to ask for permission to include this article in my dissertation.

Kind regards

Michael Kech

Dynamical Quantum Tomography

M. Kech August 24, 2016

This article is concerned with tomography schemes where the experimenter can utilize a fixed measurement setting $P \in POVM_{\mathcal{H}}$ and a known time evolution $\mathcal{T} \in CPTP_{\mathcal{H}}$ to perform (several) experiments of the following kind: Before making measurements with the setting P, the experimenter can chooses a number of time steps $k \in \mathbb{N}$ and subject the given ensemble of quantum systems prepared in state $\varrho \in \mathcal{S}(\mathcal{H})$ to the time evolution $\mathcal{T}^k$.

Particularly, given a POVM $P := \{P_1, \ldots, P_m\}$, a CPTP map $\mathcal{T} \in CPTP_{\mathcal{H}}$ and a total number of time steps $l \in \mathbb{N}_0$, the focus is on the measurement scheme

$$\mathcal{T}(P)^l := (\{P_1, \ldots, P_m\}, \ldots, \{(\mathcal{T}^*)^{l-1}(P_1), \ldots, (\mathcal{T}^*)^{l-1}(P_m)\}) \in MS_{\mathcal{H}}.$$

This article provides bounds on the number of outcomes m of the POVM P and the total number of time steps l required to allow for perfect state discrimination, also considering the scenario where prior information constrains the set of relevant quantum states to a subset of lower dimensionality.

1 Main Results

First, the focus is on unitary time evolutions. For $U \in U(\mathcal{H})$ define the CPTP map

$$\begin{aligned} \mathcal{T}_U : \mathcal{L}(\mathcal{H}) &\to \mathcal{L}(\mathcal{H}) \\ X &\mapsto UXU^\dagger. \end{aligned}$$

The article provides a subset $\mathcal{A} \subseteq U_{\mathcal{H}}$ of feasible unitaries, i.e., unitaries that are well-suited for the proposed tomography scheme. For these unitaries, the following theorem is proven.

Theorem 1 (Informationally complete tomography)**.** *Let $U \in \mathcal{A}$ be feasible. Then, for almost all POVMs P with n outcomes the measurement scheme $\mathcal{T}_U^{n+1}(P)$ is informationally complete.*

This result is optimal in the sense that there cannot be a POVM P with less outcomes such that $\mathcal{T}_U^l(P)$ is informationally complete for some $l \in \mathbb{N}$:

Proposition 2. *Let P be a POVM and let $l \in \mathbb{N}$. If $span_{\mathbb{R}}\ \mathcal{T}_U^l(P) = H(\mathcal{H})$, then P has at least n outcomes.*

The analysis can also be extended to state discrimination on subsets of the state space. Indeed, a universality theorem similar to Theorem VI.2 of [1] is proven which immediately implies the following corollaries.

Corollary 3 (Whitney)**.** *Let $U \in \mathcal{A}$ be feasible and let $\mathcal{R} \subseteq \mathcal{S}(\mathcal{H})$ be a semi-algebraic subset. Let $m \geq n$ and let $l \in \mathbb{N}$ be such that $l(m-1) > 2 \dim \mathcal{R}$. Then, for almost all POVMs P with m outcomes the measurement scheme $\mathcal{T}_U^l(P)$ is stably $\mathcal{R}$-complete.*

Corollary 4 (States of bounded rank)**.** *Let $U \in \mathcal{A}$ be feasible. Let $m \geq n$ and let $l \in \mathbb{N}$ be such that $l(m-1) \geq 4r(n-r) - 1$. Then, for almost all POVMs P with m outcomes the measurement scheme $\mathcal{T}_U^l(P)$ is stably $\mathcal{S}_r(\mathcal{H})$-complete.*

Furthermore, similar results are obtained when allowing general CPTP maps $\mathcal{T} \in CPTP_{\mathcal{H}}$. Indeed, it is shown that in this scenario POVMs with two outcomes can suffice for an informationally complete tomography and that they are also suited for state discrimination on semi-algebraic subsets of the state space.

References

[1] Michael Kech and Michael M Wolf. Quantum tomography of semi-algebraic sets with constrained measurements. *arXiv preprint arXiv:1507.00903*, 2015.

Dynamical Quantum Tomography

Michael Kech[1,*]

[1]*Department of Mathematics, Technische Universität München, 85748 Garching, Germany*

(Dated: May 22, 2016)

We consider quantum state tomography with measurement procedures of the following type: First, we subject the quantum state we aim to identify to a know time evolution for a desired period of time. Afterwards we perform a measurement with a fixed measurement set-up. This procedure can then be repeated for other periods of time, the measurement set-up however remains unaltered.

Given an n-dimensional system with suitable unitary dynamics, we show that any two states can be discriminated by performing a measurement with a set-up that has n outcomes at $n+1$ points in time.

Furthermore, we consider scenarios where prior information restricts the set of states to a subset of lower dimensionality. Given an n-dimensional system with suitable unitary dynamics and a semi-algebraic subset $\mathcal{R}$ of its state space, we show that any two states of the subset can be discriminated by performing a measurement with a set-up that has n outcomes at l steps of the time evolution if $(n-1)l \geq 2 \dim \mathcal{R}$. In addition, by going beyond unitary dynamics, we show that one can in fact reduce to a set-up with the minimal number of two outcomes.

Keywords: quantum tomography, prior information

Contents

*Electronic address: kech@ma.tum.de

I. INTRODUCTION AND SUMMARY

Quantum tomography is the task of identifying an unknown quantum state form the outcomes of a measurement. It is an integral part of quantum information science its implementation, however, is expensive. Yet, in some relevant scenarios it can be simplified: If prior information constrains the set of states to a subset of lower dimensionality the number of measurement outcomes necessary to uniquely identify a state can reduce considerably. In particular pure state tomography, or more generally tomography on states of bounded rank, has received significant attention and still is a field of active research.

Methods to find lower bounds on the number of measurement outcomes necessary to discriminate any two states of a given subset of the state space were first provided in [1] and later it was shown in [2] that these method apply in a rather general framework. However, from a practical point of view not all measurements might be feasible for implementation and thus one might want to restrict to a set of admissible measurements. Doing so, it is not clear whether the lower bounds established in [1, 2] still apply. In the context of pure state tomography it was shown in [3–6] that any two pure states can be discriminated by performing four von-Neumann measurements, which is indeed tight for systems of dimension $n \geq 5$. Additionally, in [6] this result was extended to more general subsets of the state space, including states of bounded rank. In the closely related fields of phase retrieval and low rank matrix recovery similar questions were addressed in [7–12]. Finally, at the cost of requiring slightly more measurement outcomes, robust reconstruction algorithms are provided in [13–15].

Purpose of the present paper. The conventional approach to quantum tomography is to design a certain measurement set-up. Performing a statistical experiment, the state is identified from the relative frequencies of the measurement outcomes. If the system is of dimension n, at least n^2 outcomes are required to identify an unknown state. In the present paper we consider a more general scenario. Suppose we are given a measurement set-up and that, in addition, the system can be evolved according to a know time evolution. Rather than performing a conventional measurement with the set-up, we take advantage of the time evolution by considering measurement procedures of the following kind: Having evolved the system for a desired period of time, we perform a measurement [1] with the given measurement set-up. Then, the procedure can be repeated for other periods of time. Using this measurement scheme, we show that for suitable time evolutions any state can be identified with a measurement set-up that has solely two outcomes. Furthermore, also considering the scenario where prior information constrains the relevant set of states to a subset of lower dimensionality, we provide upper bounds on the minimal number of points in time on which one has to perform a measurement in order to be able to discriminate any to states of a given subset of the state space.

In the present paper we do not consider the algorithmic problem of reconstructing the state from the measurement data.

Outline. In Section II, we fix notation and introduce notions that are relevant for the

[1] Performing a measurement should be understood as determining the relative frequencies of the measurement outcomes in the asymptotic limit of complete statistics.

following.

In Section III, we consider systems with discrete unitary dynamics. The first part is devoted to informationally complete tomography. Given the possibility to perform a measurement with a given measurement set-up at several time steps of the unitary evolution, we show that this set-up has to have at least n outcomes to perform an informationally complete tomography if the system is n-dimensional. Furthermore, we show that under some condition on the time evolution, an informationally complete tomography can be performed by measuring with a set-up that has $n+1$ outcomes at n time steps. In the second part we consider tomography on subsets of the state space. We show that performing a measurement with a set-up that has $m \geq n$ outcomes at sufficiently many points in time is a universal measurement scheme in the sense of [6]. This allows us to prove a Whitney type embedding result: Given an n-dimensional system with suitable unitary dynamics and a semi-algebraic subset $\mathcal{R}$ of its state space, we show that any two states of the subset can be discriminated by performing a measurement with a set-up that has $m \geq n$ outcomes at $l \geq \frac{2\dim \mathcal{R}}{m-1}$ steps of the time evolution. Furthermore, we show that any two states of an n-dimensional system whose rank is at most r can be discriminated by performing a measurement with a set-up that has $m \geq n$ outcomes at $l \geq \frac{4r(n-r)-1}{m-1}$ time steps. This upper bound on the number of time steps is close to the lower bound established in [1, 2].

In Section IV, we generalize the system dynamics to a larger class of discrete CPTP time evolutions. Just like in Section III we prove a universality result in the sense of [6]. Different form the case of unitary system dynamics, in this case there is just the trivial lower bound on the number of outcomes of the measurement set-up and indeed an informationally complete tomography can be performed by measuring with a set-up that has just two outcomes at $n^2 - 1$ points in time. Similar to the last section, given an n-dimensional system with suitable CPTP dynamics and a semi-algebraic subset $\mathcal{R}$ of its state space, we show that any two states of the subset can be discriminated by measuring with a set-up that has $m \geq 2$ outcomes at $l \geq \frac{2\dim \mathcal{R}}{m-1}$ steps of the time evolution. Furthermore, we show that any two state of an n-dimensional system of rank at most r can be discriminated by measuring with a measurement set-up that has $m \geq 2$ outcomes at $l \geq \frac{4r(n-r)-1}{m-1}$ steps of the time evolution.

Having solely dealt with discrete time evolutions before, in appendix B we consider the possibility of performing measurements at rational points in time of a continuous time evolution.

II. PRELIMINARIES

By $\mathcal{B}(\mathbb{C}^n)$ we denote the complex vector space of linear operators on $\mathbb{C}^n$. By $H(n)$ we denote the real vector space of hermitian operators on $\mathbb{C}^n$ and $H(n)_0$ denotes the subspace of $H(n)$ consisting of traceless hermitian operators. We equip both $H(n)$ and $\mathcal{B}(\mathbb{C}^n)$ with the Hilbert-Schmidt inner product. By $S_{H(n)_0} := \{X \in H(n)_0 : \ \|X\|_2 = 1\}$ we denote the unit sphere in $H(n)_0$ where $\|\cdot\|_2$ denotes the Hilbert-Schmidt norm. By $\mathcal{S}(\mathbb{C}^n)$ we denote the set of quantum states on $\mathbb{C}^n$, i.e. $\mathcal{S}(\mathbb{C}^n) := \{\rho \in H(n) : \rho \geq 0, \mathrm{tr}(\rho) = 1\}$. Furthermore, for a subset $A \subseteq H(n)$, we denote by $\Delta(A)$ the set of differences of operators in A, i.e. $\Delta(A) := \{X - Y : X, Y \in A\}$. By $U(n)$ we denote the set of unitary operators

on $\mathbb{C}^n$. We call a subset $A \subseteq \mathbb{R}^n$ an algebraic set if it is the real common zero locus of a set of real polynomials in n variables and we call it a semi-algebraic set if it is the set of common solutions of a finite set of real polynomial inequalities in n variables (cf. [16]).

General quantum mechanical measurements can be described by positive operator valued measures (POVMs)[17, 18]. For the purpose of the present paper we use the following definition.

Definition II.1. *(POVM.) A POVM on $\mathbb{C}^n$ is a tuple $P = (Q_1, \ldots, Q_m)$ of positive semidefinite operators on $\mathbb{C}^n$ such that*

$$\sum_{i=1}^{m} Q_i = \mathbb{1}_{\mathbb{C}^n}.$$

An element of P is called an effect operator. The dimension of P is $\dim P := |P| - 1$.

There is a linear map h_P associated to each POVM $P = (Q_1, \ldots, Q_m)$ given by

$$\begin{aligned} h_P : H(n) &\to \mathbb{R}^m \\ x &\mapsto \big(\mathrm{tr}(Q_1 x), \ldots, \mathrm{tr}(Q_m x)\big). \end{aligned}$$

A whole experiment might consist of measuring more than one POVM.

Definition II.2. *(Measurement-scheme.) A tuple of POVMs is called a measurement-scheme.*

For a tuple of natural numbers $I = (m_1, \ldots, m_l)$ let

$$\mathcal{M}(I) := \{(P^i)_{i=1}^l : \ P^i \text{ is an } m_i\text{-dimensional POVM}\}.$$

Similar to a POVM, a measurement-scheme $M = (P^1, \ldots, P^k)$ induces a linear map

$$\begin{aligned} h_M : H(n) &\to \mathbb{R}^{|P^1|+\ldots+|P^k|} \\ x &\mapsto \big(h_{P^1}(x), \ldots, h_{P^k}(x)\big). \end{aligned}$$

We equip $\mathcal{M}(I)$ with the topology induced by the metric

$$d(M, M') := \|h_M - h_{M'}\|$$

where $\|\cdot\|$ denotes the operator norm.

Definition II.3. *($\mathcal{R}$-complete.) A measurement-scheme M is called $\mathcal{R}$-complete for a subset $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ iff $h_M|_{\mathcal{R}}$ is injective. An $\mathcal{S}(\mathbb{C}^n)$-complete POVM is called informationally complete.*

Furthermore, we use the following notion of stability of measurement-schemes (cf. Definition III.2 [2]).

Definition II.4. *(Stability.) Let $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a subset and let I be a tuple of natural numbers. An $\mathcal{R}$-complete measurement-scheme $M \in \mathcal{M}(I)$ is stably $\mathcal{R}$-complete iff there exists a neighbourhood $N \subseteq \mathcal{M}(I)$ of M such that each measurement-scheme $M' \in N$ is $\mathcal{R}$-complete.*

In case the subset $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ is a smooth submanifold, the equivalence of this notion of stability to other stability properties is proven in [2].

Finally, let us define the measurement-schemes we work with in the following. Let $l \in \mathbb{N}$. For $\mathcal{T} : \mathcal{B}(\mathbb{C}^n) \to \mathcal{B}(\mathbb{C}^n)$ a unital completely positive map and $P := (Q_1, \ldots, Q_m)$ a POVM define the measurement-scheme

$$\mathcal{T}^l(P) := \Big((Q_1, \ldots, Q_m), (\mathcal{T}(Q_1), \ldots, \mathcal{T}(Q_m)), \ldots, (\mathcal{T}^{l-1}(Q_1), \ldots, \mathcal{T}^{l-1}(Q_m)) \Big). \quad (1)$$

Here the POVM P is understood to be the initial measurement set-up and $\mathcal{T}^l(P)$ is the measurement-scheme in which the POVM P is measured at l steps of the discrete time evolution described by completely positive trace preserving (CPTP) map $\mathcal{T}^\dagger$.

III. UNITARY TIME EVOLUTION

Informationally Complete Tomography

For given $U \in U(n)$ let

$$\begin{aligned} \mathcal{T}_U : \mathcal{B}(\mathbb{C}^n) &\to \mathcal{B}(\mathbb{C}^n) \\ x &\mapsto UxU^\dagger \end{aligned}$$

be the associated unital CPTP map. Furthermore, let F_U be the fix point set of $\mathcal{T}_U$, i.e. $F_U := \{X \in \mathcal{B}(\mathbb{C}^n) : \mathcal{T}_U(X) = X\}$ and let let $F_U^{sa} := \{X \in H(n) : \mathcal{T}_U(X) = X\}$. Note that we have the block decomposition $\mathcal{T}_U = \mathcal{T}_U|_{F_U} \oplus \mathcal{T}_U|_{F_U^\perp}$.

We first deal with the problem of performing informationally complete quantum tomography using a given unitary time evolution.

Proposition III.1. *Let P be a POVM and let $m \in \mathbb{N}$. If $span_{\mathbb{R}}\ \mathcal{T}_U^m(P) = H(n)$, then* $\dim P \geq n - 1$.

Proof. Let $P := (P_1, \ldots, P_k)$ be a POVM and assume $\mathrm{span}_{\mathbb{R}} \mathcal{T}_U^m = H(n)$. Clearly $\dim F_U^{sa} \geq n$ because F_U^{sa} contains the vector space of real matrices that are diagonal in a basis that diagonalizes U.

Let $\Pi_{F_U^{sa}} : H(n) \to F_U^{sa}$ be the orthogonal projection on F_U^{sa} and note that $\Pi_{F_U^{sa}} \circ \mathcal{T}_U^j(X) = \Pi_{F_U^{sa}}(X)$ for all $X \in H(n)$ and $j \in \mathbb{N}$. Therefore $F_U^{sa} = \Pi_{F_U^{sa}}(H(n)) = \Pi_{F_U^{sa}}(\mathrm{span}_{\mathbb{R}} \mathcal{T}_U^m(P)) = \mathrm{span}_{\mathbb{R}}\{\Pi_{F_U^{sa}}(P_1), \ldots, \Pi_{F_U^{sa}}(P_k)\}$ and hence $\dim F_U^{sa} \leq k$.

Combining this, we conclude $k \geq \dim F_U^{sa} \geq n$. □

Thus, to allow for an informationally complete tomography, the POVM P has to be at least $(n-1)$-dimensional. Furthermore, assuming P to be n-dimensional, one has to measure at a minimum of n points in time to achieve an informationally complete tomography and in the following we will see that this indeed suffices.

Definition III.1. *(Feasible.) A unitary matrix $U \in U(n)$ is feasible iff the algebraic multiplicity of each eigenvalue of $\mathcal{T}_U|_{F_U^\perp}$ is one and* $\dim F_U = n$.

Let us note that almost all unitaries are feasible.

Theorem III.2. *(Informationally complete tomography.) Let $U \in U(n)$ be feasible. Then, for almost all POVM P of dimension n the measurement scheme $\mathcal{T}_U^n(P)$ is informationally complete.*

The proof of this result can be found in Subsection V A.

Tomography under Prior Information

In this subsection we extend the results of the previous subsection to quantum tomography on subsets $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$.

Definition III.2. *Let $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a subset. A semi-algebraic set $\mathcal{D} \subseteq H(n)$ with $0 \notin \mathcal{D}$ represents $\Delta(\mathcal{R})$ iff for every measurement-scheme M with $h_M(X) = 0$ for some $X \in \Delta(\mathcal{R}) - \{0\}$ there exists $Y \in \mathcal{D}$ such that $h_M(Y) = 0$.*

Remark Note that a measurement-scheme M is not $\mathcal{R}$-complete if and only if there exists $X \in \Delta(\mathcal{R}) - \{0\}$ such that $h_M(X) = 0$. Thus, the set of measurement-schemes that solve the equation $h_M(Y) = 0$ for some $Y \in \mathcal{D}$ contains the set of measurement-schemes that are not $\mathcal{R}$-complete.

The next theorem is the main result of this section. It asserts that the measurement-scheme $\mathcal{T}_U^l(P)$ defined in Equation (1) is suited to perform tomography on arbitrary semi-algebraic subsets $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$.

Theorem III.3. *(Universality.) Let $U \in U(n)$ be feasible. For $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ a subset, let $\mathcal{D}$ be a semi-algebraic set that represents $\Delta(\mathcal{R})$. Let $m \geq n-1$ and let $l \in \mathbb{N}$ be such that $lm > \dim \mathcal{D}$. Then, for almost all POVM P of dimension m the measurement-scheme $\mathcal{T}_U^l(P)$ is stably $\mathcal{R}$-complete.*

The proof of this theorem can be found in Subsection V B.

In the following we discuss some consequences of Theorem III.3. First, it directly implies a Whitney type embedding result.

Corollary III.4. *(Whitney.) Let $U \in U(n)$ be feasible and let $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a subset. Let $m \geq n-1$ and let $l \in \mathbb{N}$ be such that $lm > 2 \dim \mathcal{R}$. Then, for almost all POVM P of dimension m the measurement scheme $\mathcal{T}_U^l(P)$ is stably $\mathcal{R}$-complete.*

Proof. Assume w.l.o.g. that $\mathcal{R}$ is algebraically closed, because if not we can replace $\mathcal{R}$ by its algebraic closure without changing the dimension (see Proposition 2.8.2 of [16]). By the proof of Lemma IV.2 of [6], $\Delta(\mathcal{R}) - \{0\}$ is a semi-algebraic set with $\dim \Delta(\mathcal{R}) - \{0\} \leq 2 \dim \mathcal{R}$. Applying Theorem III.3 to $\Delta(\mathcal{R}) - \{0\}$ concludes the proof. □

Theorem III.3 can also be applied to tomography on states of bounded rank. Let $\mathcal{S}_r(\mathbb{C}^n) := \{\rho \in \mathcal{S}(\mathbb{C}^n) : \mathrm{rank}(\rho) \leq r\}$ be the set of quantum states of rank at most r.

Corollary III.5. *(Tomography on states of bounded rank.) Let $U \in U(n)$ be feasible. Let $m \geq n-1$ and let $l \in \mathbb{N}$ be such that $lm \geq 4r(n-r)-1$. Then, for almost all POVM P of dimension m the measurement-scheme $\mathcal{T}_U^l(P)$ is stably $\mathcal{S}_r(\mathbb{C}^n)$-complete.*

Proof. The proof follows directly from applying Theorem III.3 to the algebraic set $\mathcal{D}$ defined in Lemma IV.6 of [6]. □

Remark If a measurement-scheme is $\mathcal{S}_r^n$-complete, it was shown in [1, 2] that, up to terms at most logarithmic in n, we have $m \geq 4r(n-r)$ and in this sense the lower bound given in Corollary III.5 is nearly optimal.

Let us note that similar to Corollary V.12 of [6], Corollary III.5 implies corresponding results for tomography on states of fixed spectrum.

IV. CPTP TIME EVOLUTION

In this section we generalize the scenario of Section III by considering a larger class of system dynamics. With this generalization the lower bound on the dimension of the initial POVM as given by Proposition III.1 can be relaxed. Indeed we show that one dimensional POVMs can suffice for informationally complete tomography and that they are also suited for tomography on subsets $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$.

Definition IV.1. *(Feasible.) A CPTP map $\mathcal{T}$ is feasible iff it is invertible and the algebraic multiplicity of each of its eigenvalues is one.*

The following result is the main result of this section. It is a universality result analogous to Theorem III.3.

Theorem IV.1. *(Universality.) Let $\mathcal{T}$ be a feasible CPTP map. For $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ a subset, let $\mathcal{D}$ be a semi-algebraic set that represents $\Delta(\mathcal{R})$. Furthermore, let $m \in \mathbb{N}$ and let $l \in \mathbb{N}$ be such that $lm > \dim \mathcal{D}$. Then, for almost all m-dimensional POVMs P the measurement-scheme $(\mathcal{T}^\dagger)^l(P)$ is stably $\mathcal{R}$-complete.*

The proof of this theorem can be found in Subsection V C. An immediate consequence is the case $k = 1$ which may be of particular interest as it shows that in fact an initial POVM of minimal dimension suffices to perform tomography on arbitrary subsets of the state space.

Corollary IV.2. *Let $\mathcal{T}$ be a feasible CPTP map. For $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ a subset, let $\mathcal{D}$ be a semi-algebraic set that represents $\Delta(\mathcal{R})$. Furthermore, let $l \in \mathbb{N}$ be such that $l > \dim \mathcal{D}$. Then, for almost all one dimensional POVM P the measurement-scheme $(\mathcal{T}^\dagger)^l(P)$ is stably $\mathcal{R}$-complete.*

Remark Given a one dimensional POVM $P := \{P_1, P_2\}$, all the relevant information is contained in P_1 as $P_2 = \mathbb{1}_{\mathbb{C}^n} - P_1$. In this sense one can identify a one dimensional POVM with an observable $O := P_1$. Under this identification the measurement-scheme $\mathcal{T}^l(P)$ corresponds to measuring the expectation value of O at l time steps of the time evolution given by $\mathcal{T}$. Corollary IV.2 then states that any two states of a given subset $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ can be discriminated by determining the expectation value of a single observable at sufficiently many time steps.

In the remainder of this section we give some further corollaries of Theorem IV.1. Of course Theorem IV.1 also covers the case of informationally complete tomography.

Corollary IV.3. *(Informationally Complete Tomography) Let $\mathcal{T}$ be a feasible CPTP map. Furthermore, let $m \in \mathbb{N}$ and let $l \in \mathbb{N}$ be such that $lm \geq n^2 - 1$. Then, for almost all m-dimensional POVM P the measurement-scheme $(\mathcal{T}^\dagger)^l(P)$ is informationally complete.*

Proof. Note that $S_{H(n)_0}$ represents $\Delta(\mathcal{S}(\mathbb{C}^n))$. Applying Theorem IV.1 to $S_{H(n)_0}$, together with the observation that $\dim S_{H(n)_0} = n - 2$, concludes the proof. □

Another immediate consequence is a Whitney type embedding result.

Corollary IV.4. *(Whitney.) Let $\mathcal{T}$ be a feasible CPTP map and let $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a subset. Furthermore, let $m \in \mathbb{N}$ and let $l \in \mathbb{N}$ be such that $lm > 2 \dim \mathcal{R}$. Then for almost all m-dimensional POVM P the measurement-scheme $(\mathcal{T}^\dagger)^l(P)$ is stably $\mathcal{R}$-complete.*

Proof. Assume w.l.o.g. that $\mathcal{R}$ is algebraically closed, because if not we can replace $\mathcal{R}$ by its algebraic closure without changing the dimension (see Proposition 2.8.2 of [16]). By the proof of Lemma IV.2 of [6], $\Delta(\mathcal{R}) - \{0\}$ is a semi-algebraic set with $\dim \Delta(\mathcal{R}) - \{0\} \leq 2 \dim \mathcal{R}$. Applying Theorem IV.1 to $\Delta(\mathcal{R}) - \{0\}$ concludes the proof. □

Finally, Theorem IV.1 can also be straightforwardly applied to tomography on states of bounded rank.

Corollary IV.5. *(Tomography on states of bounded rank.) Let $\mathcal{T}$ be a feasible CPTP map. Furthermore, let $m \in \mathbb{N}$ and let $l \in \mathbb{N}$ be such that $lm \geq 4r(n-r) - 1$. Then, for almost all POVM P of dimension m the measurement scheme $(\mathcal{T}^\dagger)^l(P)$ is stably $\mathcal{S}_r(\mathbb{C}^n)$-complete.*

Proof. The proof follows directly from applying Theorem IV.1 to the algebraic set $\mathcal{D}$ defined in Lemma IV.6 of [6]. □

V. PROOFS OF TECHNICAL RESULTS

The proofs of the following results are all based on the approach presented in [6]: Let $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ be a subset. Among all admissible measurement-schemes we characterize the subset N of non $\mathcal{R}$-complete measurement-schemes by real algebraic equations. We then prove that the subset N has a smaller dimension than the set of all admissible measurement-schemes, showing that almost all admissible measurement-schemes are $\mathcal{R}$-complete.

Denote by $\mathcal{P}(m)$ the set of m-dimensional POVMs. Let us begin by briefly discussing the measure we choose on $\mathcal{P}(m)$. Via the injective mapping

$$\eta : \mathcal{P}(m) \to (H(n))^m,\ (Q_1, \ldots, Q_{m+1}) \to (Q_1, \ldots, Q_m)$$

we can identify $\mathcal{P}(m)$ with the subset $\eta(\mathcal{P}(m))$ of $(H(n))^m$. The measure we choose on $\mathcal{P}(m)$ is the Lebesgue measure it inherits when identified with the subset $\eta(\mathcal{P}(m)) \subseteq (H(n))^m$.

A. Proof of Theorem III.2

The proof of this theorem serves as a blueprint for the other proofs presented in this section. Therefore, let us begin by giving a short outline of the proof to make our argument more transparent. Let $K = (H(n))^n$. Furthermore, observe that $\Delta(S(\mathbb{C}^n)) \subseteq H(n)_0$ and thus $H(n)_0 - \{0\}$ represents $\Delta(S(\mathbb{C}^n))$.

For $i \in \{1, \ldots, n\},\ j \in \{0, \ldots, n-1\}$ define real polynomials

$$\begin{aligned} p_{i,j} :& K \times H(n)_0 \simeq \mathbb{R}^{n^3} \times \mathbb{R}^{n^2-1} \to \mathbb{R}, \\ & (P, X) \mapsto \operatorname{tr}\left((\mathcal{T}_U)^j(Q_i)X\right) = \operatorname{tr}\left(Q_i(\mathcal{T}_U^\dagger)^j(X)\right). \end{aligned}$$

Denote by $\mathcal{V}$ the real common zero locus of the set of polynomials $\{p_{i,j}\}_{i\in\{1,\ldots,n\},\ j\in\{0,\ldots,n-1\}}$ and let

$$\mathcal{M} := (K \times (H(n)_0 - \{0\})) \cap \mathcal{V}.$$

Clearly, $\mathcal{M}$ is a semi-algebraic set and furthermore it characterizes the n-dimensional POVMs P for which $\mathcal{T}_U^n(P)$ is not informationally complete in the following sense: Let $\pi_1 : K \times H(n)_0 \to K$ denote the projection on the first factor K. Let

$$K_{NC} := \{P \in \mathcal{P}(n) : \mathcal{T}_U^n(P) \text{ is not informationally complete}\}.$$

Then, since $\eta(\mathcal{P}(n))$ is a subset of K and $H(n)_0 - \{0\}$ represents $\Delta(S(\mathbb{C}^n)) - \{0\}$, we have $\eta(K_{NC}) \subseteq \pi_1(\mathcal{M})$. We show in the following that $\dim \mathcal{M} < \dim K = n^3$. But then, by Theorem 2.8.8 of [16], we have $\dim \pi_1(\mathcal{M}) < \dim K = n^3$ and thus $\pi_1(\mathcal{M})$ has measure zero in K. Since $\eta(K_{NC})$ is a subset of $\pi_1(\mathcal{M})$, we finally conclude that $\eta(K_{NC})$ also has measure zero in K.

As a first step, we construct a decomposition of $H(n)_0$ with respect to the eigenstates of $\mathcal{T}_U^\dagger$ which allows us to simplify the analysis in the following. By changing the basis if necessary, we can assume U to be a diagonal matrix. Let $\{\lambda_{ij}\}_{i,j\in\{1,\ldots,n\}}$ [2] be the multiset of eigenvalues of $\mathcal{T}_U^\dagger$ such that for all $i, j \in \{1, \ldots, n\}$ we have

$$\mathcal{T}_U^\dagger(e_{ij}) = \lambda_{ij} e_{ij},$$

[2] Note that if $U = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, then $\lambda_{ij} = \lambda_i^* \lambda_j$ for all $i, j \in \{1, \ldots, n\}$.

where e_{ij} denotes the matrix whose only non-vanishing entry is a 1 in the i-th row and j-th column. For $k \in \mathbb{N}_0$ let

$$E_{2k} := \{X \in H(n)_0 : \mathrm{tr}(Xe_{ij}) \neq 0 \text{ for at most } 2k \text{ pairs } (i,j),\ i \neq j\}.$$

Note that $E_0 = F_U \cap H(n)_0$ since U is feasible by assumption.

Proposition V.1. *E_{2k} is an algebraic set with $\dim E_k = n - 1 + 2k$.*

Proof. Let $C := \{(i,j) \in \mathbb{N}^2 : i > j\}$. For $S \subseteq C$ let $N(S) := \{X \in H(n)_0 :\ \mathrm{tr}(Xe_s) = 0,\ \forall s \in S\}$. $N(S)$ is a linear subspace and thus clearly an algebraic set. Furthermore, let $(j,l) \in C$ and note that $e_{jl} = (e_{jl} + e_{lj}) + i(-ie_{jl} + ie_{lj})$. Thus, for a hermitian matrix $X \in H(n)_0$ we have $\mathrm{tr}(Xe_{jl}) = 0$ if and only if $\mathrm{tr}\,(X(e_{jl} + e_{lj}))$ and $\mathrm{tr}\,(X(ie_{jl} - ie_{lj})) = 0$. The matrices $\{e_{jl} + e_{lj}, ie_{jl} - ie_{lj}\}_{(j,l)\in C} \subseteq H(n)_0$ are linearly independent and hence $\dim N(S) = n^2 - 1 - 2|S|$. But $E_{2k} = \bigcup_{S\subseteq C, |S| = \frac{n^2-n}{2} - k} N(S)$. Hence, as a finite union of algebraic sets, E_{2k} is an algebraic set and furthermore $\dim E_k = n^2 - 1 - 2(\frac{n^2-n}{2} - k) = n - 1 + 2k$. □

Let $R_0 := E_0 - \{0\}$. For $k \in \{1, \ldots, \lceil n/2 \rceil - 1\}$ [3] let $R_k := E_{2k} - E_{2k-2}$ be the set of hermitian matrices with precisely $2k$ non-vanishing off-diagonal entries and let $R_{\lceil n/2 \rceil} := H(n)_0 - E_{2\lceil n/2 \rceil - 2}$. Observe that $R_{\lceil n/2 \rceil}$ might be empty and that $H(n)_0 - \{0\} = \bigcup_{k=0}^{\lceil n/2 \rceil} R_k$.

Furthermore, for $k \in \{0, \ldots, \lceil n/2 \rceil\}$, let $\mathcal{M}_k := (K \times R_k) \cap \mathcal{V}$ and observe that

$$\mathcal{M} = \bigcup_{k=0}^{\lceil n/2 \rceil} \mathcal{M}_k.$$

Hence, to complete the proof of Theorem III.2, it suffices to prove the following proposition.

Proposition V.2. *Let $k \in \{0, \ldots, \lceil n/2 \rceil\}$. Then $\dim \mathcal{M}_k < \dim K$.*

Proof. Let $R_k^1 := \{X \in R_k :\ \mathrm{tr}(XE_0) = 0\}$ and $R_k^2 = R_k - R_k^1$ [4]. Going along the lines of the proof of Proposition V.1, it is seen that that $\dim R_k^1 = 2k$. For $i \in \{1,2\}$ let $\mathcal{M}_k^i := (K \times R_k^i) \cap \mathcal{V}$ and note that $\mathcal{M}_k = \mathcal{M}_k^1 \cup \mathcal{M}_k^2$.

In a first step, we prove that $\dim \mathcal{M}_k^2 < \dim K$. In order to do so we prove the following proposition as an intermediate step.

Proposition V.3. *For $X \in R_k^2$, the set of matrices $\{(\mathcal{T}_U^\dagger)^j(X)\}_{j\in\{0,\ldots,2k\}}$ is linearly independent over $\mathbb{C}$.*

Proof. First note that by construction of R_k^2 there is an $i \in \{1, \ldots, n\}$ such that $0 \neq \mathrm{tr}(Xe_{ii}) =: X_0$. Furthermore, by construction of R_k, there are distinct eigenvectors $e_{i_1 j_1}, \ldots, e_{i_{2k} j_{2k}}$ such that for all $m \in \{1, \ldots, 2k\}$ we have $i_m \neq j_m$ and $0 \neq \mathrm{tr}(Xe_{i_m j_m}) =: X_m$. Let $Y = \mathrm{span}_{\mathbb{C}}(\{e_{ii}\} \cup \{e_{i_m j_m}\}_{m\in\{1,\ldots,2k\}})$ [5] and let $\pi_Y : \mathcal{B}(\mathbb{C}^n) \to Y$

[3] Here $\lceil x \rceil :=$ smallest integer greater than x.
[4] Note that $R_0^1 = \emptyset$.
[5] Note that $\{e_{ii}\} \cup \{e_{i_m j_m}\}_{m\in\{1,\ldots,2k\}}$ indeed is an orthonormal basis of Y.

be the orthogonal projection on Y. It is enough to show that $\left\{\pi_Y\left((\mathcal{T}_U^\dagger)^j(X)\right)\right\}_{j\in\{0,\dots,2k\}}$ is a set linearly independent operators over $\mathbb{C}$. Consider the $(2k+1)\times(2k+1)$ matrix $M := \left(\mathrm{tr}\left(\pi_Y\left((\mathcal{T}_U^\dagger)^l(X)\right)e_{i_mj_m}\right)\right)_{l,m=0}^{2k}$, where $e_{i_0j_0}=e_{ii}$. The determinant of M is proportional to the determinant of the Vandermonde matrix whose entries are determined by the eigenvalues of $\mathcal{T}_U^\dagger$:

$$
\begin{aligned}
&\det(M)\\
&= \det\begin{bmatrix} X_0 & X_0 & \dots & X_0 \\ \lambda^0_{i_1j_1}X_1 & \lambda^1_{i_1j_1}X_1 & \dots & \lambda^{2k}_{i_1j_1}X_1 \\ \vdots & \vdots & & \vdots \\ \lambda^0_{i_{2k}j_{2k}}X_{2k} & \lambda^1_{i_{2k}j_{2k}}X_{2k} & \dots & \lambda^{2k}_{i_{2k}j_{2k}}X_{2k}\end{bmatrix} = X_0\cdot\ldots\cdot X_{2k}\ \det\begin{bmatrix} 1 & 1 & \dots & 1 \\ \lambda^0_{i_1j_1} & \lambda^1_{i_1j_1} & \dots & \lambda^{2k}_{i_1j_1} \\ \vdots & \vdots & & \vdots \\ \lambda^0_{i_{2k}j_{2k}} & \lambda^1_{i_{2k}j_{2k}} & \dots & \lambda^{2k}_{i_{2k}j_{2k}}\end{bmatrix}\\
&= \frac{X_0\cdot\ldots\cdot X_{2k}}{\lambda_{i_1j_1}\cdot\ldots\cdot\lambda_{i_{2k}j_{2k}}}\ \det\begin{bmatrix} 1 & 1 & \dots & 1 \\ \lambda^1_{i_1j_1} & \lambda^2_{i_1j_1} & \dots & \lambda^{2k+1}_{i_1j_1} \\ \vdots & \vdots & & \vdots \\ \lambda^1_{i_{2k}j_{2k}} & \lambda^2_{i_{2k}j_{2k}} & \dots & \lambda^{2k+1}_{i_{2k}j_{2k}}\end{bmatrix}\\
&= \frac{X_0\cdot\ldots\cdot X_{2k}}{\lambda_{i_1j_1}\cdot\ldots\cdot\lambda_{i_{2k}j_{2k}}}\prod_{0\le o<p\le m}(\lambda_{i_pj_p}-\lambda_{i_oj_0}),
\end{aligned}
$$

where $\lambda_{i_0j_0}=1$. Since U is a unitary matrix, we have $\lambda_{i_mj_m}\neq 0$ for all $m\in\{1,\dots,2k\}$. Furthermore, since U is feasible by assumption, $\lambda_{i_lj_l}\neq\lambda_{i_mj_m}$ for all $m,l\in\{0,\dots,2k\}$ with $m\neq l$. This, together with $X_m\neq 0,\ m\in\{0,\dots,2k\}$, shows that $\det(M)\neq 0$ and hence proves the claim. □

Now let $X\in R_k^2$ be fixed. From the previous proposition we conclude that at least $n\cdot\min\{(2k+1),n\}$ of the linear equations

$$\mathrm{tr}\left(Q_i(\mathcal{T}_U^\dagger)^j(X)\right)=0,\ i\in\{1,\dots,n\},\ j\in\{0,\dots,n-1\},\ (Q_1,\dots,Q_n)\in K, \qquad (2)$$

are independent. Hence the dimension of the solution set of the equations (2) is by at least $n\cdot\min\{2k+1,n\}$ smaller than the dimension of K. Since this holds for all $X\in R_k^2$ we find

$$
\begin{aligned}
\dim\mathcal{M}_k^2 &\le \dim K+\dim R_k^2-n(2k+1)=\dim K+n-1+2k-n(2k+1)\\
&\le \dim K-2(n-1)k-1<\dim K
\end{aligned}
$$

if $k\in\{0,\dots,[n/2]-1\}$ using Proposition V.1 and furthermore

$$
\begin{aligned}
\dim\mathcal{M}_{[n/2]}^2 &\le \dim K+\dim H(n)_0-n^2=\dim K+n^2-1-n^2\\
&= \dim K-1<\dim K.
\end{aligned}
$$

In the second step we show that $\dim\mathcal{M}_k^1<n^3$ [6]. Let $X\in R_k^1$ be fixed. By going along the lines of the proof of Proposition V.3 it follows that the smaller set of operators

[6] Note that we can restrict to $k>0$ since $R_0^1=\emptyset$.

$\{(\mathcal{T}_U^\dagger)^j(X)\}_{j\in\{0,\ldots,2k-1\}}$ still is linearly independent over $\mathbb{C}$ [7]. We conclude that at least $n\cdot\min\{2k,n\}$ of the linear equations

$$\mathrm{tr}\left(Q_i(\mathcal{T}_U^\dagger)^j(X)\right)=0,\ i\in\{1,\ldots,n\},\ j\in\{0,\ldots,n-1\},\ (Q_1,\ldots,Q_n)\in K, \tag{3}$$

are independent. Thus, the dimension of the solution set of the equations (3) is by at least $n\cdot\min\{2k,n\}$ smaller than the dimension of K. Since this holds for all $X\in R_k^1$ we find

$$\begin{aligned}\dim\mathcal{M}_k^1 &\leq \dim K+\dim R_k^1-n(2k)=\dim K+2k-2nk\\ &\leq \dim K-2(n-1)k<\dim K\end{aligned}$$

if $k\in\{1,\ldots,\lceil n/2\rceil-1\}$ and furthermore

$$\begin{aligned}\dim\mathcal{M}_{\lceil n/2\rceil}^1 &\leq \dim K+\dim H(n)_0-n^2=\dim K+n^2-1-n^2\\ &=\dim K-1<\dim K.\end{aligned}$$

Finally, since $\mathcal{M}_k=\mathcal{M}_k^1\cup\mathcal{M}_k^2$, we conclude $\dim\mathcal{M}_k<\dim K$. □

B. Proof of Theorem III.3

Let $K=(H(n))^m$ [8]. Define the semi-algebraic map ϕ by

$$\begin{aligned}\phi: H(n)_0-\{0\}&\to S_{H(n)_0}\\ x&\mapsto\frac{x}{\|x\|_2}.\end{aligned} \tag{4}$$

Let $\mathcal{D}$ be the semi-algebraic set that represents $\Delta(\mathcal{R})$, then $\phi(\mathcal{D})$ represents $\Delta(\mathcal{R})$ by Proposition 2.2.7 of [16] and $\dim\phi(\mathcal{D})\leq\dim\mathcal{D}$ by Theorem 2.8.8 of [16]. $S_{H(n)_0}$ is closed in the norm topology and by Proposition 2.8.2 of [16] the dimension of a semi-algebraic set coincides with the dimension of its closure in the norm topology. We conclude that the closure $\overline{\phi(\mathcal{D})}$ of $\phi(\mathcal{D})$ is a subset of $S_{H(n)_0}$ with $\dim\overline{\phi(\mathcal{D})}\leq\dim\mathcal{D}$. In addition, by Proposition 2.2.2 of [16], $\overline{\phi(\mathcal{D})}$ is semi-algebraic and hence represents $\Delta(\mathcal{R})$. In the following we replace $\mathcal{D}$ by $\overline{\phi(\mathcal{D})}$ if $\mathcal{D}$ is not a closed subset of $S_{H(n)_0}$.

For the most part, the remainder of this proof can be straightforwardly obtained by going along the lines of the proof of Theorem III.2. However, for the sake of completeness, let us give the whole argument.

For $k\in\{0,1,\ldots,\lceil l/2\rceil-1\}$, let $\mathcal{D}_k^i:=\mathcal{D}\cap R_k^i,\ i=1,2$, and note that we have $\dim\mathcal{D}_k^1\leq 2k-1$(if $k>1$) and $\dim\mathcal{D}_k^2\leq n-2+2k$ [9]. Let $\mathcal{D}_{\lceil l/2\rceil}:=\mathcal{D}-\bigcup_{k=0}^{\lceil l/2\rceil-1}(\mathcal{D}_k^1\cup\mathcal{D}_k^2)$ and let

[7] Considering $X\in R_k^1$ in the proof of Proposition V.3 just corresponds to setting $X_0=0$. The remainder of the argument still applies.

[8] Just like in the last subsection, we identify the set of m-dimensional POVMs on $\mathbb{C}^n$ with the semi-algebraic subset $\eta(\mathcal{P}(m))$ of $(H(n))^m$.

[9] We get the upper bounds $2k-1$ and $n-2+2k$ rather then $2k$ and $n-1+2k$. This is because $\mathcal{D}\subseteq S_{H(n)_0}$ and $\dim(E_k\cap S_{H(n)_0})=n-2+2k+1$ as can be seen from the proof of propositions V.1 and V.4.

$\mathcal{D}^1_{[l/2]} := \{X \in \mathcal{D}_{[l/2]} : \operatorname{tr}(XE_0) = 0\}$, $\mathcal{D}^2_{[l/2]} = \mathcal{D}_{[l/2]} - \mathcal{D}^1_{[l/2]}$. Note that $\dim \mathcal{D}^i_{[l/2]} \leq \dim \mathcal{D}$ for $i = 1, 2$. Also note that $\mathcal{D} = \bigcup_{j=1}^{[l/2]} (\mathcal{D}^1_j \cup \mathcal{D}^2_j)$.

Just like in the proof of Theorem III.2, for $j \in \{0, \ldots, l-1\},\ i \in \{1, \ldots, m\}$, define real polynomials

$$\begin{aligned} p_{i,j} :& K \times H_0(n) \simeq \mathbb{R}^{mn^2} \times \mathbb{R}^{n^2-1} \to \mathbb{R}, \\ & (P, X) \mapsto \operatorname{tr}\left(Q_i (\mathcal{T}_U^\dagger)^j (X)\right). \end{aligned}$$

Denote by $\mathcal{V}$ the common zero locus of the polynomials $\{p_{i,j}\}_{j \in \{0,\ldots,l-1\},\ i \in \{1,\ldots,m\}}$ and for $i \in \{1, 2\}$, $k \in \{0, 1, \ldots, \lceil l/2 \rceil\}$, let $\mathcal{M}^i_k := (K \times \mathcal{D}^i_k) \cap \mathcal{V}$.

First we prove that for all $k \in \{0, 1, \ldots, \lceil l/2 \rceil\}$ we have $\dim \mathcal{M}^2_k < \dim K$. So let $k \in \{0, \ldots, \lceil l/2 \rceil\}$. If $\mathcal{D}^2_k = \emptyset$ we have $\mathcal{M}^2_k = \emptyset$ and thus we clearly have $\dim \mathcal{M}^2_k < \dim K$. Otherwise let $X \in \mathcal{D}^2_k$ be fixed. From Proposition V.3 we conclude that at least $m \cdot \min\{2k+1, l\}$ of the linear equations

$$\operatorname{tr}\left(Q_i (\mathcal{T}_U^\dagger)^j (X)\right) = 0,\ j \in \{0, \ldots, l-1\},\ i \in \{1, \ldots, m\},\ (Q_1, \ldots, Q_m) \in K, \tag{5}$$

are independent. Hence the dimension of the solution set of the equations (5) is by at least $m \cdot \min\{2k+1, l\}$ smaller than the dimension of K. Since this holds for all $X \in \mathcal{D}^2_k$ we find

$$\begin{aligned} \dim \mathcal{M}^2_k &\leq \dim K + \dim \mathcal{D}^2_k - m(2k+1) \leq \dim K + n - 2 + 2k - m(2k+1) \\ &= \dim K - (m - (n-1)) - 2k(m-1) - 1 < \dim K \end{aligned}$$

for $k \in \{0, \ldots, [l/2] - 1\}$, using the assumption that $m \geq n - 1$. Also by assumption we have $\dim \mathcal{D} < ml$ and thus $\dim \mathcal{D}^2_{[l/2]} \leq \dim \mathcal{D} < ml$. Hence we conclude that

$$\begin{aligned} \dim \mathcal{M}^2_{[l/2]} &\leq \dim K + \dim \mathcal{D} - ml \\ &< \dim K + ml - ml = \dim K. \end{aligned}$$

Next we prove that for all $k \in \{1, \ldots, \lceil l/2 \rceil\}$ we have $\dim \mathcal{M}^1_k < \dim K$. So let $k \in \{1, \ldots, \lceil l/2 \rceil\}$. If $\mathcal{D}^1_k = \emptyset$ we have $\mathcal{M}^1_k = \emptyset$ and thus clearly $\dim \mathcal{M}^1_k < \dim K$. Otherwise let $X \in \mathcal{D}^1_k$ be fixed. From Proposition V.3 we conclude that at least $m \cdot \min\{2k, l\}$ of the linear equations

$$\operatorname{tr}\left(Q_i (\mathcal{T}_U)^j (X)\right) = 0,\ j \in \{0, \ldots, l-1\},\ i \in \{1, \ldots, m\},\ (Q_1, \ldots, Q_m) \in K, \tag{6}$$

are independent. Hence the dimension of the solution set of the equations (6) is by at least $m \cdot \min\{2k, l\}$ smaller than the dimension of K. Since this holds for all $X \in \mathcal{D}^1_k$ we find

$$\begin{aligned} \dim \mathcal{M}^1_k &\leq \dim K + \dim \mathcal{D}^1_k - m(2k) = \dim K + 2k - 1 - 2mk \\ &= \dim K - 2k(m-1) - 1 < \dim K \end{aligned}$$

for $k \in \{1, \ldots, [l/2] - 1\}$. Using $\dim \mathcal{D}^1_{[l/2]} \leq \dim \mathcal{D} < ml$ we also conclude that

$$\begin{aligned} \dim \mathcal{M}^1_{[l/2]} &\leq \dim K + \dim \mathcal{D} - ml \\ &< \dim K + ml - ml = \dim K. \end{aligned}$$

Finally, let $\pi_1 : K \times H(n)_0 \to K$ be the projection on the first factor K and let $\mathcal{M} := \bigcup_{k=0}^{\lceil l/2 \rceil} (\mathcal{M}_k^1 \cup \mathcal{M}_k^2)$. Clearly, $\mathcal{M}$ is a semi-algebraic set. Let

$$K_{\mathcal{R}} := \{P \in \mathcal{P}(m) : \mathcal{T}_U^l(P) \text{ is not } \mathcal{R}-\text{complete.}\}.$$

Then, since $\eta(\mathcal{P}(m))$ is a subset of K and $\mathcal{D}$ represents $\Delta(\mathcal{R})$, we have $\eta(K_{\mathcal{R}}) \subseteq \pi_1(\mathcal{M})$. We have shown that for all $i \in \{1,2\}$, $k \in \{0,\ldots,\lceil l/2 \rceil\}$ we have $\dim \mathcal{M}_k^i < \dim K$ and thus $\dim \mathcal{M} < \dim K$. Hence we find $\dim \pi_1(\mathcal{M}) < \dim K$ by Theorem 2.8.8 of [16]. But since $\eta(K_{\mathcal{R}})$ is a subset of $\pi_1(\mathcal{M})$, we conclude that $\eta(K_{\mathcal{R}})$ has measure zero in K.

Finally, since $\mathcal{D}$ is a closed subset of $S_{H(n)_0}$, the stability follows form Lemma IV.1 of [6].

C. Proof of Theorem IV.1

Just like in the proof of Theorem III.3, we replace $\mathcal{D}$ by $\overline{\phi(\mathcal{D})}$ if $\mathcal{D}$ is not a closed subset of $S_{H(n)_0}$.

Again, the remainder of this proof is close to the proof of Theorem III.2. Let $\{\mathbb{1}, e_1, \ldots, e_{n^2-1}\}$ be the set of eigenvectors of $\mathcal{T}^\dagger$. For $k \in \mathbb{N}_0$ let

$$D_k := \{X \in S_{H(n)_0} : \mathrm{tr}(Xe_i) \neq 0 \text{ for at most } k \text{ elements } i \in \{1,\ldots,n^2-1\}\}.$$

Proposition V.4. *For $k \in \{1,\ldots,n^2-1\}$, D_k is an algebraic set of dimension at most $k-1$.*

Proof. For $A \subseteq \{1,\ldots,n^2-1\}$ let $N(A) := \{X \in \mathcal{B}(\mathbb{C}^n) : \mathrm{tr}(X) = 0 \wedge \forall i \in S : \mathrm{tr}(Xe_i) = 0\}$ and note that $\dim_{\mathbb{C}} N(A) = n^2 - 1 - |A|$ since the set of operators $\{\mathbb{1}, e_1, \ldots, e_{n^2-1}\}$ is linearly independent over $\mathbb{C}$. From this it follows that for all $A \subseteq \{1,\ldots,n^2-1\}$ we have $\dim(N(A) \cap H(n)_0) \leq n^2 - 1 - |A|$: Assume for a contradiction that $\dim(N(A) \cap H(n)_0) = m > n^2 - 1 - |A|$. Then there are is a set $\{h_1,\ldots,h_m\} \subseteq H(n)_0 \subseteq N(A)$ of linearly independent operators over $\mathbb{R}$. Being a set of hermitian operators, $\{h_1,\ldots,h_m\}$ is also linearly independent over $\mathbb{C}$ and hence we conclude that $\dim N(A) \geq m$, a contradiction. Now note that $D_k = \left(\bigcup_{A \subseteq \{1,\ldots,n^2-1\} : |A| = n^2-1-k} N(A)\right) \cap S_{H(n)_0}$. Thus D_k is a real algebraic set and $\dim D_k \leq \left(n^2 - 1 - (n^2 - 1 - k)\right) - 1 = k - 1$.

□

For $k \in \mathbb{N}$ let $Q_k := D_k - D_{k-1}$. For $k \in \{1,\ldots,l-1\}$ let $\mathcal{D}_k := \mathcal{D} \cap Q_k$ and note that $\mathcal{D}_k$ is a semi-algebraic set with $\dim \mathcal{D}_k \leq k-1$. Furthermore let $\mathcal{D}_l := \mathcal{D} - \bigcup_{k=1}^{l-1} \mathcal{D}_k$ and note that $\dim \mathcal{D}_l \leq \dim \mathcal{D}$. Then we have $\bigcup_{k=1}^{l} \mathcal{D}_k = \mathcal{D}$.

Let $K := (H(n))^m$ [10]. Just like in the proof of Theorem III.2, for $j \in \{0,\ldots,l-1\}$, $i \in \{1,\ldots,m\}$, define real polynomials

$$\begin{aligned} p_{i,j} : K \times H_0(n) \simeq \mathbb{R}^{mn^2} \times \mathbb{R}^{n^2-1} &\to \mathbb{R}, \\ (P, X) &\mapsto \mathrm{tr}\left(Q_i(\mathcal{T})^j(X)\right). \end{aligned}$$

[10] Just like in Subsection V A, we identify the set of m-dimensional POVMs on $\mathbb{C}^n$ with the semi-algebraic subset $\eta(\mathcal{P}(m))$ of $(H(n))^m$.

Denote by $\mathcal{V}$ the common zero locus of the polynomials $\{p_{i,j}\}_{j\in\{0,\ldots,l-1\},\ i\in\{1,\ldots,m\}}$ and set $\mathcal{M}_k := (K \times \mathcal{D}_k) \cap \mathcal{V}$ for $k \in \{1,\ldots,l\}$.

Next we prove that for all $k \in \{1,\ldots,l\}$ we have $\dim \mathcal{M}_k < \dim K$. So let $k \in \{1,\ldots,l\}$. If $\mathcal{D}_k = \emptyset$ we have $\mathcal{M}_k = \emptyset$ and thus we clearly have $\dim \mathcal{M}_k < \dim K$. Otherwise let $X \in \mathcal{D}_k$ be fixed. Using feasibility of the map $\mathcal{T}$, it is seen, by going along the lines of the proof of Proposition V.3, that the set of operators $\{(\mathcal{T})^i(X)\}_{i\in\{0,\ldots,k-1\}}$ is linearly independent over $\mathbb{C}$. This implies that at least $m \cdot k$ of the linear equations

$$\operatorname{tr}\left(Q_i \mathcal{T}^j(X)\right) = 0,\ j \in \{0,\ldots,l-1\},\ i \in \{1,\ldots,m\},\ (Q_1,\ldots,Q_m) \in K, \tag{7}$$

are independent. Hence the dimension of the solution set of the equations (7) is by at least $m \cdot k$ smaller than the dimension of K. Since this holds for all $X \in \mathcal{D}_k^1$ we find

$$\begin{aligned}\dim \mathcal{M}_k &\leq \dim K + \dim \mathcal{D}_k - km \leq \dim K + (k-1) - km \\ &\leq \dim K - (m-1)k - 1 < \dim K\end{aligned}$$

for $k < l$. For $k = l$ we find

$$\begin{aligned}\dim \mathcal{M}_k &\leq \dim K + \dim \mathcal{D}_l - lm \leq \dim K + \dim \mathcal{D} - lm \\ &< \dim K + lm - lm < \dim K,\end{aligned}$$

where we used the assumption that $lm > \dim \mathcal{D}$.

Let $\pi_1 : K \times H(n)_0 \to K$ be the projection on the first factor K and let $\mathcal{M} := \bigcup_{k=1}^{l} \mathcal{M}_k$. Clearly, $\mathcal{M}$ is a semi-algebraic set. Let

$$K_{\mathcal{R}} := \{P \in \mathcal{P}(m) : (\mathcal{T}^\dagger)^l(P) \ \text{ is not } \mathcal{R}-\text{complete.}\}.$$

Then, since $\eta(\mathcal{P}(m)) \subseteq K$ and $\mathcal{D}$ represents $\Delta(\mathcal{R})$, we have $\eta(K_{\mathcal{R}}) \subseteq \pi_1(\mathcal{M})$. We have shown that $\dim \mathcal{M}_k < \dim K$ for all $k \in \{1,\ldots,l\}$ and thus $\dim \mathcal{M} < \dim K$. Hence we find $\dim \pi_1(\mathcal{M}) < \dim K$ by Theorem 2.8.8 of [16]. But since $\eta(K_{\mathcal{R}})$ is a subset of $\pi_1(\mathcal{M})$, this implies that $\eta(K_{\mathcal{R}})$ has measure zero in K.

Finally, since $\mathcal{D}$ is a closed subset of $S_{H(n)_0}$, stability follows form Lemma IV.1 of [6].

Appendix A: Continuous Time Evolution

In this appendix we consider continuous dynamics generated by Lie semigroups. Let $\mathcal{L} : \mathcal{B}(\mathbb{C}^n) \to \mathcal{B}(\mathbb{C}^n)$ be a unital conditional completely positive map generating the one parameter family of unital CP maps $\mathcal{T}_t := e^{t\mathcal{L}} : \mathcal{B}(\mathbb{C}^n) \to \mathcal{B}(\mathbb{C}^n)$ where $t \in \mathbb{R}_0^+$.

Instead of measuring the initial POVM after equidistant time steps of the system dynamics given by $\mathcal{T}_t$ we now consider more general time steps. More precisely, for $T := (t_1,\ldots,t_l)$ a tuple of rational numbers such that $0 < t_1 < t_2 < \ldots < t_l < 1$ and $P := (Q_1,\ldots,Q_m)$ a POVM define the measurement-scheme

$$\mathcal{L}_T(P) := \left((P_1,\ldots,P_m),(\mathcal{T}_{t_1}(P_1),\ldots,\mathcal{T}_{t_1}(P_m)),\ldots,(\mathcal{T}_{t_l}(P_1),\ldots,\mathcal{T}_{t_l}(P_m))\right).$$

To obtain generalizations of Theorem III.3 and Theorem IV.1 it suffices to generalize Proposition V.3 to rational points in time, the remainder of their proofs can be transferred.

For $T := (t_1, \ldots, t_l) \in \mathbb{Q}^l$ such that $0 < t_1 < t_2 < \ldots < t_l < 1$ and $\Lambda := \{\lambda_1, \ldots, \lambda_l\} \subseteq \mathbb{C} - \{0, 1\}$ a subset define

$$V_T^\Lambda := \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \lambda_1^{t_1} & \ldots & \lambda_1^{t_l} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_l^{t_1} & \ldots & \lambda_l^{t_l} \end{pmatrix}.$$

Proposition A.1. *V_T^Λ is invertible.*

Proof. Let $N, m_1, \ldots, m_l \in \mathbb{N}$ be such that $t_i = \frac{m_i}{N}$. Extend Λ to a set $\tilde{\Lambda} := \{\lambda_1, \ldots, \lambda_{m_l}\} \subseteq \mathbb{C} - \{0, 1\}$. Let $\tilde{\lambda}_i := \lambda_i^{\frac{1}{N}}$, $i \in \{1, \ldots, m_l\}$. Then $\det V_T^\Lambda$ is a minor of the matrix

$$V := \begin{pmatrix} 1 & 1 & \ldots & 1 & \ldots & 1 \\ 1 & \tilde{\lambda}_1 & \ldots & \tilde{\lambda}_1^{m_1} & \ldots & \tilde{\lambda}_1^{m_l} \\ \vdots & \vdots & & \vdots & & \vdots \\ 1 & \tilde{\lambda}_{m_1} & \ldots & \tilde{\lambda}_{m_1}^{m_1} & \ldots & \tilde{\lambda}_{m_1}^{m_l} \\ \vdots & \vdots & & \vdots & & \vdots \\ 1 & \tilde{\lambda}_{m_l} & \ldots & \tilde{\lambda}_{m_l}^{m_1} & \ldots & \tilde{\lambda}_{m_l}^{m_l} \end{pmatrix}.$$

Multiplying V from the left with the diagonal matrix $\mathrm{Diag}(\tilde{\lambda}_1, \ldots, \tilde{\lambda}_{m_l})$ gives a Vandermonde matrix. This Vandermonde matrix is totally non-singular since $\tilde{\Lambda} \subseteq \mathbb{C} - \{0, 1\}$ by construction. Thus $\det V_T^\Lambda$ does not vanish. □

From Proposition A.1 we directly obtain the following generalizations of Theorem III.3 and Theorem IV.1 respectively.

Corollary A.2. *Let $T := (t_1, \ldots, t_l) \in \mathbb{Q}^l$ such that $0 < t_1 < \ldots < t_l < 1$. Let $h \in H(n)$ be such that e^{ih} is feasible. For $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ a subset, let $\mathcal{D}$ be a semi-algebraic set that represents $\Delta(\mathcal{R})$. Let $m \geq n - 1$ and let $l \in \mathbb{N}$ be such that $(l + 1)m > \dim \mathcal{D}$, then for almost all POVM P of dimension m, the measurement scheme $\mathcal{T}_U^l(P)$ is stably $\mathcal{R}$-complete.*

Corollary A.3. *Let $T := (t_1, \ldots, t_l) \in \mathbb{Q}^l$ such that $0 < t_1 < \ldots < t_l < 1$. Let $\mathcal{L}$ be a unital conditional completely positive map such that $e^{\mathcal{L}}$ is feasible. For $\mathcal{R} \subseteq \mathcal{S}(\mathbb{C}^n)$ a subset, let $\mathcal{D}$ be a semi-algebraic set that represents $\Delta(\mathcal{R})$. Let $m \in \mathbb{N}$ and let $l \in \mathbb{C}$ be such that $(l+1)m > \dim \mathcal{D}$, then for almost all m-dimensional POVM P, the measurement scheme $\mathcal{T}^l(P)$ is stably $\mathcal{R}$-complete.*

---

[1] Teiko Heinosaari, Luca Mazzarella, and Michael M Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318(2):355–374, 2013.

[2] Michael Kech, Péter Vrana, and Michael Wolf. The role of topology in quantum tomography. *Journal of Physics A: Mathematical and Theoretical*, 48(26):265303, 2015.

[3] Damien Mondragon and Vladislav Voroninski. Determination of all pure quantum states from a minimal number of observables. *arXiv preprint arXiv:1306.1214*, 2013.

[4] Philippe Jaming. Uniqueness results in an extension of pauli's phase retrieval problem. *Applied and Computational Harmonic Analysis*, 37(3):413–441, 2014.

[5] Claudio Carmeli, Teiko Heinosaari, Jussi Schultz, and Alessandro Toigo. How many orthonormal bases are needed to distinguish all pure quantum states? *arXiv preprint arXiv:1504.01590*, 2015.

[6] Michael Kech and Michael Wolf. Quantum tomography with natural povms. *to appear*.

[7] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Applied and Computational Harmonic Analysis*, 20(3):345–356, 2006.

[8] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. *Applied and Computational Harmonic Analysis*, 2014.

[9] Dan Edidin. Projections and phase retrieval. *arXiv preprint arXiv:1506.00674*, 2015.

[10] Cynthia Vinzant. A small frame and a certificate of its injectivity. *arXiv preprint arXiv:1502.04656*, 2015.

[11] Richard Kueng, Holger Rauhut, and Ulrich Terstiege. Low rank matrix recovery from rank one measurements. *arXiv preprint arXiv:1410.6913*, 2014.

[12] Zhiqiang Xu. The minimal measurement number for low-rank matrices recovery. *arXiv preprint arXiv:1505.07204*, 2015.

[13] David Gross. Recovering low-rank matrices from few coefficients in any basis. *IEEE Trans. on Information Theory*, 57:1548–1566, 2011.

[14] Steven T Flammia, David Gross, Yi-Kai Liu, and Jens Eisert. Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators. *New Journal of Physics*, 14(9):095022, 2012.

[15] D. Gross, F. Krahmer, and R. Kueng. A partial derandomization of phaselift using spherical designs. *arXiv:1310.2267*, 2013.

[16] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*. Springer, 1998.

[17] Alexander S Holevo. *Probabilistic and statistical aspects of quantum theory*, volume 1. Springer, 2011.

[18] Paul Busch, Marian Grabowski, and Pekka Johannes Lahti. *Operational quantum physics*, volume 31. Springer, 1995.