The role of general quantum measurements in information technologies

An inaugural dissertation

submitted for the degree of Dr. rer. nat.
in the Faculty of Mathematics and Natural Sciences
at the Heinrich Heine University Düsseldorf

presented by

Felix Bischof
born in Siegen

Düsseldorf, August 2019

From the Institute for Theoretical Physics III
at the Heinrich Heine University Düsseldorf

Published by permission of the
Faculty of Mathematics and Natural Sciences at the
Heinrich Heine University Düsseldorf

Supervisor: PD Dr. Hermann Kampermann

Co-supervisor: Prof. Dr. Dagmar Bruß

Date of the oral examination: 30.09.2019

Abstract

Quantum information theory explores the opportunities and challenges that arise when quantum systems are used as information carriers. However, the interface of most information technologies (e.g., in cryptography and computing) is classical and this data is obtained via a measurement of the quantum system. Therefore, general quantum measurements (also called POVMs) play a central role in information technologies.

While the understanding of noiseless, projective measurements is advanced in the literature, the role of noisy, general measurements is an active research field. It is known that due to their rich structure POVMs outperform projective measurements for numerous tasks in quantum information theory. This is because the noise present in a measurement can be a valuable resource rather than a drawback. In this thesis, we introduce and investigate two different information-theoretic scenarios and study the role of general quantum measurements in them.

First, we consider *quantum randomness generation*. Random numbers are an integral part of many information-theoretical tasks, in particular cryptography. Measurements of quantum systems enable the generation of bit strings that are truly unpredictable for any observer. We devise and analyze a general measurement-device-independent randomness generation setup, consisting of a well-characterized source of quantum states and a completely uncharacterized and untrusted detector. Moreover, we provide a semidefinite program that allows to quantify the cryptographic randomness gain of any such setup via efficient numerical computation. This is used to propose simple and realistic quantum random number generators that yield high randomness generation rates for detectors who exhibit the statistics of general quantum measurements.

Second, we introduce and analyze a *resource theory of coherence based on general quantum measurements*. Quantum coherence is a fundamental feature of quantum states and a prerequisite for the advantage of quantum information technologies. We devise a generalized, rigorous, resource-theoretical framework which defines quantum coherence (superposition) with respect to a general measurement. In particular, we characterize quantum states and quantum operations that are free of the coherence resource. A semidefinite program is used to compute interconversion properties of resource states. We present several POVM-based coherence measures that generalize well-known standard coherence measures, and study their properties and relations. In addition, we establish a connection of POVM-based coherence to randomness generation: under a mild assumption, a fundamental POVM-coherence measure is equal to the cryptographic randomness gain. This provides an important operational meaning to our resource theory.

Zusammenfassung

Die Quanteninformationstheorie untersucht die neuen Möglichkeiten und Herausforderungen, die entstehen, wenn Quantensysteme als Informationträger dienen. Die Benutzeroberfläche der meisten Informationstechnologien (z.B. in der Kryptographie und im Computing) ist jedoch klassisch und diese Daten werden durch eine Messung des Quantensystems gewonnen. Daher spielen allgemeine Quantenmessungen (auch POVMs genannt) eine zentrale Rolle in Quanten-Informationstechnologien.

Während das Verständnis von rauschfreien, projektiven Messungen weit fortgeschritten ist, ist die Rolle von verrauschten, allgemeinen Messungen ein Gegenstand der aktuellen Forschung. Aufgrund ihrer komplexen Struktur übertreffen POVMs projektive Messungen in vielen Anwendungen der Quanteninformationstheorie. Daher ist das (Quanten-)Rauschen in allgemeinen Messungen nicht immer ein Nachteil, sondern eine potenziell wertvolle Ressource. In dieser Dissertation werden zwei unterschiedliche informationstheoretische Szenarien im besonderen Hinblick auf die Rolle von allgemeinen Quantenmessungen untersucht.

Das erste Thema ist die *Quanten-Zufallszahlenerzeugung*. Zufallszahlen sind ein integraler Bestandteil vieler informationstheoretischer Anwendungen, insbesondere der Kryptographie. Das Messen von Quantensystemen ermöglicht die Erzeugung von Zeichenfolgen, die für jeden Beobachter unvorhersagbar sind. Wir formulieren und analysieren ein allgemeines messgerät-unabhängiges Schema zur Erzeugung von Zufallszahlen, bestehend aus einer genau charakterisierten Quantenzustands-Quelle und einem uncharakterisierten und nicht vertrauenswürdigen Detektor. Darüber hinaus zeigen wir ein semidefinites Programm, das die effiziente numerische Quantifizierung der kryptographischen Zufallsrate ermöglicht. Dadurch sind wir in der Lage einfache und realistische Schemata zu entwerfen, die hohe Zufallsraten garantieren, für Detektoren, deren Statistik allgemeinen Quantenmessungen entspricht.

Das zweite Thema ist die Konstruktion und Analyse einer *Ressourcentheorie der Kohärenz basierend auf allgemeinen Quantenmessungen*. Kohärenz ist eine fundamentale Eigenschaft von Quantenzuständen und eine grundlegende Bedingung für die meisten Anwendungen der Quanteninformationstheorie. Wir konstruieren ein verallgemeinertes, mathematisch rigoroses Modell, in dem die Ressource Kohärenz (Superposition) definiert wird bezüglich einer allgemeinen Messung. Insbesondere charakterisieren wir ressourcenfreie Quantenzustände und Quantenkanäle. Ein semidefinites Programm ermöglicht die Bestimmung von Konvertierungseigenschaften von Ressourcen-Zuständen. Wir führen mehrere POVM-Kohärenzmaße ein, die bisherige Ressourcenmaße der Standard-Kohärenztheorie verallgemeinern, und untersuchen deren Eigenschaften. Ferner beweisen wir einen Zusammen-

hang zwischen POVM-Kohärenz und Zufallszahlenerzeugung: in einem wichtigen Spezialfall entspricht ein fundamentales POVM-Kohärenzmaß genau der kryptographischen Zufallsrate. Dieses Resultat etabliert eine operative Bedeutung unserer Ressourcentheorie.

Acknowledgments

This thesis would not have been possible without the fortunate environment of people that I encountered.

First and foremost, I want to thank my main supervisor, Hermann Kampermann. His door was always open to offer support and advice on problems of any kind. His mathematical intuition and confident knowledge in abstract problems were of great help and inspired me in my work. Furthermore, I am very grateful to Dagmar Bruß for taking me in her group and her contribution to shape me into a scientist. I wish to thank both of my supervisors for valuable feedback and advice in numerous scientific discussions.

I am grateful to all members of the Institute for Theoretical Physics III, past and present, for providing a very pleasant working environment. In particular, I wish to thank Timo Holz for making it the enjoyable experience it was. Moreover, my sincere thanks go to Junyi Wu, Michael Epping, Jochen Szangolies, Sarnava Datta, Federico Grasselli, Giulio Gianfelici, Carlo Liorni, Lucas Tendick and Gláucia Murta. In addition, I very much appreciate the help in proofreading this manuscript provided by Sarnava Datta, Giulio Gianfelici, Federico Grasselli, Timo Holz, Carlo Liorni and Daniel Miller.

I gratefully acknowledge the support I received from Evangelisches Studienwerk Villigst. Their generous scholarship made this dissertation possible. In their network, I experienced the other scholarship recipients as very pleasant and stimulating people. I also thank the German Federal Ministry of Education and Research (BMBF) for funding.

My high school physics teacher, Karl-Günter Hilger, spurred my interest in physics through great teaching and I thank him for that. My passion for this subject also developed because of numerous friends in Dormagen, Zürich and Düsseldorf.

I express my gratitude to all of the authors of the publications in the references. I met only a few of them in person, but their works shaped my thinking.

Finally and most importantly, I wish to thank my parents, my sisters and my wider family for their continuous loving support.

Contents

CHAPTER 1

Introduction

The laws of *quantum mechanics* govern the behavior of physical systems at the smallest scales in nature. Predictions of quantum mechanics have been verified in experiment to an extremely high degree of accuracy [OHdG06]. In this thesis, we restrict our attention to finite-dimensional and non-relativistic quantum systems. In particular, we focus on discrete time steps, that is, on individiual states, measurements and evolutions with distinguished properties. Finally, we consider quantum mechanics from the viewpoint of *information theory* – a framework founded by Claude Shannon [Sha48] to quantitatively describe the storage and communication of information.

The intersection of quantum mechanics and information theory has been proven to be very fruitful. In the beginning of the 20th century, the features of quantum mechanics, e.g., its inherent uncertainty, puzzled the physics community [EPR35]. In *quantum information theory*, these features are understood as a valuable resource rather than a drawback. This led to the invention of *quantum information technologies*, i.e., practical applications of quantum mechanics, which aim at surpassing restrictions in information processing imposed by classical physics. Among other examples, this includes the celebrated tasks of *quantum cryptography* [SBPC$^+$09], *quantum computing* [NC00, LJL$^+$10] and *quantum randomness generation* [AM16]. Moreover, the information-theoretical viewpoint of quantum mechanics allows us to comprehend the abstract mathematical quantum formalism from a deeper and more physical perspective.

Any quantum experiment is necessarily composed of the preparation of a state and the measurement of it. Measurements take a more prominent role in quantum mechanics than in classical physics, as in the latter there is no need to introduce observables through measurements. Consequently, measurements play an integral part in quantum information technologies. In the open system formulation of quantum mechanics, systems can be noisy which enables to describe (the lack of) information. Noisy quantum measurements are also called general quantum measurements or positive-operator-valued measures (POVMs) [Hel69]. The latter name stems from the fact that POVMs are described by conditions similar to probability measures. Interestingly, POVMs can outperform projective measurements for many tasks in quantum information theory [OGWA17]. This includes quantum

tomography [RBKSC04], unambiguous discrimination of quantum states [Ber10], quantum cryptography [Ben92, Ren04], Bell inequalities [Gis96, VB10] or quantum randomness generation [APVW16, BKB17].

In this thesis, we present new insights into the role of general quantum measurements in information technologies. Our work is organized as follows. The subsequent four chapters are devoted to providing all mathematical tools and concepts for the in-depth understanding of the results. In particular, they contain selected findings that are not detailed in our included publications. In Chap. 2 we present tools from linear algebra that are extensively used in this work. In particular, we describe concepts such as partial isometries and the generalized inverse, which are not necessarily contained in textbooks. In Chap. 3 we introduce noisy quantum mechanics from the perspective of finite-dimensional information theory. This formulation is particularly suited to introduce quantum information concepts. Chapter 4 describes how the constituents of quantum mechanics can be purified in order to be free of noise. In Chap. 5 we introduce semidefinite programming and provide selected applications that will be used in this work. This includes semidefinite programs for the optimization over measurements and quantum channels under particular constraints.

The following two chapters contain the main results of this thesis. In Chap. 6 we describe and investigate quantum randomness generation. We focus on a measurement-device-independent randomness generation setup and present our findings. Chap. 7 describes the quantum resource theory of coherence. There, we present results on our resource theory of coherence based on general quantum measurements. Finally, in Chap. 8 we conclude and give an outlook for possible future research directions.

The Appendix contains supplementary information. In App. A we include the original publications used for this thesis, as well as publication details. In App. B we provide Matlab files that implement functions and semidefinite programs related to our work.

CHAPTER 2

Elements of Linear Algebra

The (finite-dimensional) Hilbert space formalism of quantum mechanics is formulated in the language of linear algebra. This section serves as a summary of important concepts and results in linear algebra that are used throughout the thesis. It is assumed that the reader is familiar with basic concepts of linear algebra that can be found in many introductory textbooks, which includes the concepts of vector space, basis, matrix representation, eigenvalues and scalar product. The content is mostly based on the two books on linear algebra by Fischer [Fis03] and Jänich [Jän08]. Additionally, Renner's lecture notes [Ren13], Tomamichel's thesis [Tom12] and the book *Quantum Computation and Quantum Information* by Nielsen and Chuang [NC00] were used as resources.

2.1 Hilbert Spaces

A finite-dimensional *Hilbert space* $\mathcal{H}$ is a finite-dimensional vector space over the complex numbers equipped with a *scalar product* $\langle \cdot | \cdot \rangle \colon \mathcal{H} \times \mathcal{H} \to \mathbb{C}$. We use the convention that the scalar product is conjugate-linear in its first argument, $\alpha\langle\phi|\psi\rangle = \langle\alpha^*\phi|\psi\rangle = \langle\phi|\alpha\psi\rangle$, for any $\phi, \psi \in \mathcal{H}$ and where α^* denotes the complex conjugation of any $\alpha \in \mathbb{C}$. The *dual space* $\mathcal{H}^*$ is the vector space of all linear forms on $\mathcal{H}$, that is, linear functions from $\mathcal{H}$ to $\mathbb{C}$. In the Dirac *bra-ket notation*, elements of $\mathcal{H}$ are denoted by kets $|\psi\rangle$, while elements of $\mathcal{H}^*$ are denoted by bras $\langle\phi|$. The scalar product provides a one-to-one correspondence between kets and bras. Concretely, to any $|\psi\rangle \in \mathcal{H}$ we associate $\langle\psi| \in \mathcal{H}^*$ via the *vector space isomorphism* (from now on just isomorphism)

$$|\psi\rangle \mapsto \langle\psi|(\cdot) \coloneqq \langle\psi| \cdot \rangle \in \mathcal{H}^*. \tag{2.1}$$

In the following, we make extensive use of this correspondence by which we can write $\langle\phi||\psi\rangle \coloneqq \langle\phi|(|\psi\rangle) = \langle\phi|\psi\rangle$ for any ket and bra.

The scalar product introduces a measure of lengths and angles on the Hilbert space. A vector $|\psi\rangle \in \mathcal{H}$ is *normalized* if it has length one, $\langle\psi|\psi\rangle = 1$. We call a set of kets $\{|\psi_i\rangle\}$ *orthogonal* if $\langle\psi_i|\psi_j\rangle = 0$ for all $i \neq j$, and we call it *orthonormal* if additionally all vectors are normalized. The orthonormality condition can be conveniently written as $\langle\psi_i|\psi_j\rangle = \delta_{i,j}$ with the Kronecker symbol $\delta_{i,j}$.

Given a set of kets $\{|e_i\rangle \in \mathcal{H}\}$, its complex (real) *span*, denoted $\mathrm{span}_{\mathbb{C}}\{|e_i\rangle\}$ ($\mathrm{span}_{\mathbb{R}}\{|e_i\rangle\}$), is the subspace of all complex (real) linear combinations of the vectors $|e_i\rangle$. A *basis* $\{|b_i\rangle\}$ of $\mathcal{H}$ is an ordered set of vectors (we always employ lexicographical ordering) such that any vector $|\psi\rangle \in \mathcal{H}$ can be written as a unique linear combination of the basis. With that, the *dimension* of $\mathcal{H}$, denoted $\dim \mathcal{H}$, is defined as the number of elements of a basis. The set $\{|b_i\rangle\}$ forms a basis if and only if it is *linearly independent* and $\mathrm{span}_{\mathbb{C}}\{|b_i\rangle\} = \mathcal{H}$. Consequently, an orthogonal set $\{|e_i\rangle\}$ with $\mathrm{span}_{\mathbb{C}}\{|e_i\rangle\} = \mathcal{H}$ is a basis of $\mathcal{H}$.

2.1.1 Direct Sum and Tensor Product

Two subspaces $S, S' \subseteq \mathcal{H}$ of a Hilbert space $\mathcal{H}$ are orthogonal, denoted $S \perp S'$, if $\langle s|s'\rangle = 0$ holds for all $|s\rangle \in S$ and all $|s'\rangle \in S'$. For such subspaces, their *orthogonal direct sum* is defined as

$$S \oplus S' = \{|s\rangle + |s'\rangle : |s\rangle \in S, |s'\rangle \in S', S \perp S'\}. \tag{2.2}$$

We will often omit the word orthogonal when talking about orthogonal direct sums. The dimension of the direct sum is given by $\dim(S \oplus S') = \dim S + \dim S'$. The *orthogonal complement* of S in $\mathcal{H}$ is the unique subspace $S^{\perp}$ such that $S \oplus S^{\perp} = \mathcal{H}$.

Given two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the *tensor product* $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined as the linear span of all (formal) pairs $|\psi\rangle \otimes |\psi'\rangle$, where $|\psi\rangle \in \mathcal{H}_A$ and $|\psi'\rangle \in \mathcal{H}_B$, such that the following relations hold

- $(\alpha|\psi\rangle) \otimes |\psi'\rangle = |\psi\rangle \otimes (\alpha|\psi'\rangle) = \alpha|\psi\rangle \otimes |\psi'\rangle$
- $(|\psi_1\rangle + |\psi_2\rangle) \otimes |\psi'\rangle = |\psi_1\rangle \otimes |\psi'\rangle + |\psi_2\rangle \otimes |\psi'\rangle$
- $|\psi\rangle \otimes (|\psi_1'\rangle + |\psi_2'\rangle) = |\psi\rangle \otimes |\psi_1'\rangle + |\psi\rangle \otimes |\psi_2'\rangle$

for any $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_A$, $|\psi_1'\rangle, |\psi_2'\rangle \in \mathcal{H}_B$, and $\alpha \in \mathbb{C}$. Moreover, the scalar product on $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined by the sesquilinear extension of

$$\langle \psi_1 \otimes \psi_1' | \psi_2 \otimes \psi_2' \rangle = \langle \psi_1 | \psi_2 \rangle \langle \psi_1' | \psi_2' \rangle \tag{2.3}$$

to all elements of $\mathcal{H}_A \otimes \mathcal{H}_B$. For orthonormal bases $\{|e_i\rangle\}_i$ of $\mathcal{H}_A$ and $\{|e_j'\rangle\}_j$ of $\mathcal{H}_B$, the set $\{|e_i\rangle \otimes |e_j'\rangle\}_{i,j}$ is an orthonormal basis of $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\dim(\mathcal{H}_A \otimes \mathcal{H}_B) = \dim \mathcal{H}_A \cdot \dim \mathcal{H}_B$.

2.2 Linear Operators on Hilbert spaces

The set of *linear operators* from $\mathcal{H}$ to $\mathcal{H}'$ is also a vector space, denoted by $\mathrm{L}(\mathcal{H}, \mathcal{H}')$. Of particular importance are (rank-one) operators $R \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ that can be written as the concatenation of a bra $\langle\beta| \in \mathcal{H}^*$ and a ket $|\alpha\rangle \in \mathcal{H}'$ as

$$R(\cdot) = |\alpha\rangle\langle\beta|(\cdot) \coloneqq \langle\beta| \cdot \rangle|\alpha\rangle. \tag{2.4}$$

In particular, for orthonormal bases $\{|e_j\rangle\}_j$ of $\mathcal{H}$ and $\{|e'_i\rangle\}_i$ of $\mathcal{H}'$, the set of operators $\{|e'_i\rangle\langle e_j|\}_{i,j}$ is a basis of $\mathrm{L}(\mathcal{H},\mathcal{H}')$. Every operator $L \in \mathrm{L}(\mathcal{H},\mathcal{H}')$ can be represented as a matrix in this basis,

$$L = \sum_{i,j} \langle e'_i|L|e_j\rangle |e'_i\rangle\langle e_j|, \tag{2.5}$$

where $L_{i,j} = \langle e'_i|L|e_j\rangle$ denotes the (i,j)-entry of the matrix.

For every $L \in \mathrm{L}(\mathcal{H},\mathcal{H}')$ the *adjoint* operator $L^\dagger \in \mathrm{L}(\mathcal{H}',\mathcal{H})$ is the unique operator satisfying

$$\langle \phi|L\psi\rangle = \langle L^\dagger\phi|\psi\rangle \tag{2.6}$$

for any $\psi \in \mathcal{H}$ and $\phi \in \mathcal{H}'$ (omitting Dirac notation). This definition is equivalent to $\langle\phi|L|\psi\rangle = \langle\psi|L^\dagger|\phi\rangle^*$, for any $|\psi\rangle \in \mathcal{H}$ and $|\phi\rangle \in \mathcal{H}'$. In matrix notation, the adjoint operator of $(L_{i,j})_{i,j}$ is obtained by taking the conjugate transpose, that is, $(L^\dagger_{i,j})_{i,j} = (L^*_{j,i})_{i,j}$.

We will now define important subspaces that can be associated to every linear operator. They are visualized in Fig. 2.1. The *kernel* of an operator $L \in \mathrm{L}(\mathcal{H},\mathcal{H}')$ is defined as the subspace of vectors that are mapped to zero, namely

$$\ker(L) = \{|\psi\rangle \in \mathcal{H} : L|\psi\rangle = 0\}. \tag{2.7}$$

Closely related is the *support* of L, being the orthogonal complement of the kernel $\mathrm{supp}(L) = (\ker L)^\perp$. Further, the *image* of L is the subspace of $\mathcal{H}'$ spanned by (the columns of) L

$$\mathrm{im}(L) = \{L|\psi\rangle : |\psi\rangle \in \mathcal{H}\}. \tag{2.8}$$

With that, the *rank* of L is given as the dimension of its image, $\mathrm{rank}\, L = \dim(\mathrm{im}\, L) = \dim(\mathrm{supp}\, L)$. Taking the adjoint exchanges image and support of any $L \in \mathrm{L}(\mathcal{H},\mathcal{H}')$, i.e., $\mathrm{supp}\, L^\dagger = \mathrm{im}\, L$ and $\mathrm{im}\, L^\dagger = \mathrm{supp}\, L$. Finally, the restriction of a linear operator $L \in \mathrm{L}(\mathcal{H},\mathcal{H}')$ to a subspace $S \subseteq \mathcal{H}$ is by definition the linear map

$$\begin{aligned} L|_S &: S \to \mathcal{H}' \\ \text{such that } &|s\rangle \mapsto L|s\rangle \text{ for all } |s\rangle \in S. \end{aligned} \tag{2.9}$$

Conversely, when we specify the action of a linear operator $L \in \mathrm{L}(\mathcal{H},\mathcal{H}')$ only on a subspace $S \subseteq \mathcal{H}$, we mean that $L|_{S^\perp} = 0$.

2.2.1 Projectors, Isometries and Generalized Inverse

The set of linear operators from $\mathcal{H}$ to itself is denoted by $\mathrm{L}(\mathcal{H}) \coloneqq \mathrm{L}(\mathcal{H},\mathcal{H})$. Its elements are called endomorphism and have a square matrix representation. The

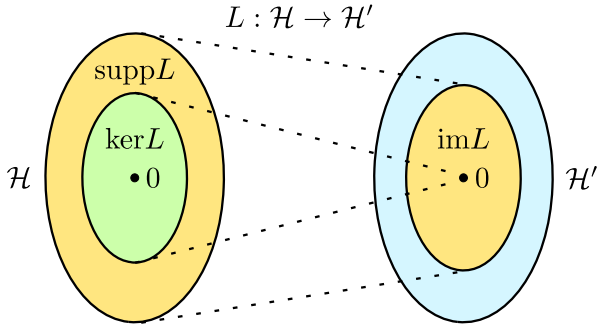

Figure 2.1: Important subspaces that can be associated to every linear operator $L \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$. The kernel of L is the subspace $\ker(L) \subseteq \mathcal{H}$ that gets mapped to zero. Its orthogonal complement $(\ker L)^\perp = \mathrm{supp}(L)$ is called the support of L. The image of L is the subspace $\mathrm{im}(L) \subseteq \mathcal{H}'$ that is spanned by L.

orthogonal projection onto a subspace S is an operator $P \in \mathrm{L}(\mathcal{H})$ with $\mathrm{supp}\, P = \mathrm{im}\, P = S$ that acts as an identity on S, i.e., $P|_S = \mathbb{1}_S$. This implies that $P^2 = P$ and $P^\dagger = P$, and conversely, every operator $P \in \mathrm{L}(\mathcal{H})$ with these two properties is an orthogonal projection. In the following, we denote the projector onto S by Π_S. This operator can be decomposed in any orthonormal basis $\{|e_i\rangle\}$ of S as $\Pi_S = \sum_{i=1}^{\dim S} |e_i\rangle\langle e_i|$. This holds in particular for the *identity* operator $\mathbb{1} = \Pi_{\mathcal{H}}$. The projector onto $S^\perp$ is then given by $\Pi_{S^\perp} = \mathbb{1} - \Pi_S$.

The *inverse* of an operator $L \in \mathrm{L}(\mathcal{H})$, if it exists, is the unique operator $L^{-1} \in \mathrm{L}(\mathcal{H})$ satisfying $L^{-1}L = LL^{-1} = \mathbb{1}$. For singular or non-square operators we use the *generalized inverse* (Moore-Penrose inverse), which exists for every operator $L \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ and is defined as the inverse of L on its support. More precisely, the generalized inverse $L^- \in \mathrm{L}(\mathcal{H}', \mathcal{H})$ of L is the unique operator satisfying $L^- L = \Pi_{\mathrm{supp}\, L}$ and $\mathrm{supp}\, L^- = \mathrm{im}\, L$.

Operators $V \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ that preserve the scalar product of any two vectors are of particular importance in quantum mechanics. These are called *isometries* and are defined as

$$\langle V\phi | V\psi \rangle = \langle \phi | \psi \rangle \tag{2.10}$$

for any $\phi, \psi \in \mathcal{H}$ (omitting Dirac notation). The definition is equivalent to $\langle V^\dagger V\phi | \psi \rangle = \langle V\phi | V\psi \rangle = \langle \phi | \psi \rangle$, i.e., $V^\dagger V = \mathbb{1}$. This means, a linear map $V \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ is an isometry if and only if it maps an orthonormal basis $\{|e_i\rangle\}$ of $\mathcal{H}$ to an orthonormal set $\{|e_i'\rangle \in \mathcal{H}'\}$, i.e., $V|e_i\rangle = |e_i'\rangle$. In matrix notation, V is an isometry if and only if its columns form an orthonormal set. A *unitary* operator $U \in \mathrm{L}(\mathcal{H})$ is an isometry from $\mathcal{H}$ to itself. Because of $U^\dagger U = \mathbb{1}$, the inverse of a unitary operator U exists and is given by the adjoint $U^{-1} = U^\dagger$. A more general concept, the *partial isometry* is an operator $V \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ that satisfies

$V^\dagger V = \Pi_{\operatorname{supp} V}$. Hence, its generalized inverse is equal to the adjoint $V^- = V^\dagger$ and is also a partial isometry. Furthermore, the restricted partial isometry $V|_{\operatorname{supp} V}$ is an isometry between $\operatorname{supp} V \subseteq \mathcal{H}$ and $\mathcal{H}'$. Thus, an isometry is a partial isometry with full support on $\mathcal{H}$. Since isometries preserve angles and distances, they can be understood as embeddings. Let $\mathcal{H}$ and $\mathcal{H}'$ be two Hilbert spaces such that $\dim \mathcal{H} \leq \dim \mathcal{H}'$ and let $V \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ be an isometry that embeds $\mathcal{H}$ into $\mathcal{H}'$, i.e., it satisfies $V^\dagger V = \mathbb{1}$ on $\mathcal{H}$. Then, for every operator $L \in \mathrm{L}(\mathcal{H})$, we define its embedding by isometric conjugation $L' \coloneqq VLV^\dagger \in \mathrm{L}(\mathcal{H}')$. In particular, L' has the same nonzero eigenvalues as L (see Sec. 2.3).

2.2.2 Partial Trace

The set of linear operators $\mathrm{L}(\mathcal{H}, \mathcal{H}')$ is a vector space and thus we can form the tensor product $\mathrm{L}(\mathcal{H}_A, \mathcal{H}'_A) \otimes \mathrm{L}(\mathcal{H}_B, \mathcal{H}'_B)$, as defined in the previous section. One can show that there exists a canonical identification (isometry) of this space with the space of linear operators from $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}'_A \otimes \mathcal{H}'_B$, that is,

$$\mathrm{L}(\mathcal{H}_A, \mathcal{H}'_A) \otimes \mathrm{L}(\mathcal{H}_B, \mathcal{H}'_B) \simeq \mathrm{L}(\mathcal{H}_A \otimes \mathcal{H}_B, \mathcal{H}'_A \otimes \mathcal{H}'_B). \tag{2.11}$$

This correspondence allows us to write

$$(L \otimes R)(|\psi_A\rangle \otimes |\psi_B\rangle) = (L|\psi_A\rangle) \otimes (R|\psi_B\rangle) \tag{2.12}$$

for any two operators $L \in \mathrm{L}(\mathcal{H}_A, \mathcal{H}'_A)$, $R \in \mathrm{L}(\mathcal{H}_B, \mathcal{H}'_B)$, and $|\psi_A\rangle \in \mathcal{H}_A$, $|\psi_B\rangle \in \mathcal{H}_B$. An analogous property can be used to define the direct sum of operators defined on subspaces $S, S' \subseteq \mathcal{H}$,

$$(L \oplus R)(|s\rangle \oplus |s'\rangle) \coloneqq (L|s\rangle) \oplus (R|s'\rangle) \tag{2.13}$$

for given operators $L \in \mathrm{L}(S, \mathcal{H}')$, $R \in \mathrm{L}(S', \mathcal{H}')$ and any $|s\rangle \in S$, $|s'\rangle \in S'$.

The *trace* of a (square) operator $L \in \mathrm{L}(\mathcal{H})$ over a Hilbert space $\mathcal{H}$ is defined by

$$\operatorname{tr}(L) \coloneqq \sum_i \langle e_i|L|e_i\rangle \tag{2.14}$$

where $\{|e_i\rangle\}$ is any orthonormal basis of $\mathcal{H}$. Hence, in matrix notation the trace is obtained by summing all diagonal elements. The trace is well-defined because the above expression is independent of the basis choice, which can be seen as follows. Let $\{|e'_i\rangle\}$ be any orthonormal basis which implies $\mathbb{1} = \sum_j |e'_j\rangle\langle e'_j|$. Then, $\operatorname{tr}(L) = \sum_{i,j} \langle e_i|L|e'_j\rangle\langle e'_j|e_i\rangle = \sum_{i,j} \langle e'_j|e_i\rangle\langle e_i|L|e'_j\rangle = \sum_j \langle e'_j|L|e'_j\rangle$. The trace operation $\operatorname{tr}\colon \mathrm{L}(\mathcal{H}) \to \mathbb{C}$ is linear, i.e.,

$$\operatorname{tr}(\alpha L + \beta R) = \alpha \operatorname{tr}(L) + \beta \operatorname{tr}(R), \tag{2.15}$$

for any $L, R \in \mathrm{L}(\mathcal{H})$ and $\alpha, \beta \in \mathbb{C}$. Further properties of the trace operation are

- $\mathrm{tr}(L^\dagger) = \mathrm{tr}(L)^*$
- $\mathrm{tr}(LR) = \mathrm{tr}(RL)$ (*cyclicity*)
- $\mathrm{tr}(VLV^\dagger) = \mathrm{tr}(L)$ for any isometry V,

where the third property follows immediately from the second.

The *partial trace* tr_B is a map from operators $\mathrm{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ on a product space $\mathcal{H}_A \otimes \mathcal{H}_B$ to the operators $\mathrm{L}(\mathcal{H}_A)$ on $\mathcal{H}_A$. It is defined by the linear extension of the mapping

$$\mathrm{tr}_B : L \otimes R \mapsto \mathrm{tr}(R)L \tag{2.16}$$

for any $L \in \mathrm{L}(\mathcal{H}_A)$ and $R \in \mathrm{L}(\mathcal{H}_B)$. Similar to the trace operation, the partial trace tr_B is linear and commutes with taking the adjoint. Furthermore, it obeys the two important properties

$$\mathrm{tr}_B(R(L \otimes \mathbb{1})) = \mathrm{tr}_B(R)L \tag{2.17}$$

$$\mathrm{tr}_B((L \otimes \mathbb{1})R) = L\,\mathrm{tr}_B(R) \tag{2.18}$$

where $R \in \mathrm{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $L \in \mathrm{L}(\mathcal{H}_A)$. Finally, the trace over a bipartite system can be decomposed into partial traces over the individual systems, $\mathrm{tr}(R) = \mathrm{tr}(\mathrm{tr}_B(R))$.

2.3 Operator Decompositions

Certain classes of operators in $\mathrm{L}(\mathcal{H}, \mathcal{H}')$ have decompositions that are useful in applications. First, we discuss how this vector space can be equipped with a scalar product and discuss hermitian operators. The *Hilbert-Schmidt scalar product* on the complex vector space $\mathrm{L}(\mathcal{H}, \mathcal{H}')$ is defined as

$$\langle L, R\rangle \coloneqq \mathrm{tr}(L^\dagger R) \tag{2.19}$$

for any operators $L, R \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$. For orthonormal bases $\{|e_j\rangle\}_j$ of $\mathcal{H}$ and $\{|e'_i\rangle\}_i$ of $\mathcal{H}'$, the basis $\{|e'_i\rangle\langle e_j|\}_{i,j}$ of $\mathrm{L}(\mathcal{H}, \mathcal{H}')$ is orthonormal with respect to the Hilbert-Schmidt scalar product. Consider the tensor space $\mathcal{H}' \otimes \mathcal{H}$ equipped with the basis $\mathcal{B} = \{|e'_i\rangle \otimes |e_j\rangle\}$. The linear map $\mathrm{vec}_\mathcal{B}$ given by

$$\mathrm{vec}_\mathcal{B}(|e'_i\rangle\langle e_j|) = |e'_i\rangle \otimes |e_j\rangle \tag{2.20}$$

is an isomorphism between $\mathrm{L}(\mathcal{H}, \mathcal{H}')$ and $\mathcal{H}' \otimes \mathcal{H}$, and an isometry because it maps an orthonormal basis onto another. Therefore it has the property

$$\langle \mathrm{vec}(L)|\,\mathrm{vec}(R)\rangle = \langle L, R\rangle \tag{2.21}$$

for any $L, R \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$, which can also be verified directly. We employ in Eq. (2.20) the *row vectorization* convention, while also the column vectorization convention is frequently used [WBC15].

2.3.1 Hermitian and Positive Operators

An operator $M \in \mathrm{L}(\mathcal{H})$ is called *hermitian* if $M^\dagger = M$. The set of hermitian matrices $\mathrm{H}(\mathcal{H})$ is closed under addition of matrices and multiplication with real numbers and hence forms a real subspace (subspace over $\mathbb{R}$) of $\mathrm{L}(\mathcal{H})$. Moreover, equipped with the Hilbert-Schmidt scalar product from Eq. (2.19), it is a real Hilbert space. For an orthonormal basis $\{|e_i\rangle\}$ of $\mathcal{H}$, the set of operators $E_{i,j}$ defined by

$$E_{i,j} \coloneqq \begin{cases} \frac{1}{\sqrt{2}}(|e_i\rangle\langle e_j| + |e_j\rangle\langle e_i|) & \text{if } i < j \\ \frac{i}{\sqrt{2}}(|e_i\rangle\langle e_j| - |e_j\rangle\langle e_i|) & \text{if } i > j \\ |e_i\rangle\langle e_i| & \text{otherwise} \end{cases} \tag{2.22}$$

forms a Hilbert-Schmidt orthonormal basis of $\mathrm{H}(\mathcal{H})$. Therefore, its real dimension is given by $\dim_{\mathbb{R}} \mathrm{H}(\mathcal{H}) = (\dim_{\mathbb{C}} \mathcal{H})^2$.

An operator $M \in \mathrm{L}(\mathcal{H})$ is called *positive semidefinite* if

$$\langle\psi|M|\psi\rangle \geq 0 \quad \text{for all } |\psi\rangle \in \mathcal{H}. \tag{2.23}$$

Note, that in the following we call M from (2.23) simply *positive*, and we call it *strictly positive* if the expectation values are strictly greater than zero. The set $\mathrm{P}(\mathcal{H})$ of positive operators is a subset of $\mathrm{H}(\mathcal{H})$ and we often write $M \geq 0$ to indicate that $M \in \mathrm{P}(\mathcal{H})$. Moreover, given two hermitian operators $M, N \in \mathrm{H}(\mathcal{H})$, the notation $M \geq N$ means that $M - N \geq 0$. For any two positive operators $M, N \geq 0$, the trace of their product cannot be negative, $\mathrm{tr}(MN) \geq 0$. Finally, an operator M is positive if and only if there exists an operator $L \in \mathrm{L}(H)$ such that $M = L^\dagger L$. The "if" direction holds because $\langle\psi|L^\dagger L|\psi\rangle = \langle\psi'|\psi'\rangle \geq 0$, where $|\psi'\rangle = L|\psi\rangle$. The "only if" direction holds because every positive operator M has a uniqe positive square root $\sqrt{M}$, which can be obtained from the spectral decomposition in the next section, Eq. (2.24).

2.3.2 Spectral Decomposition

An operator $L \in \mathrm{L}(\mathcal{H})$ is called *normal* if it commutes with its adjoint, i.e., $L^\dagger L = LL^\dagger$. Among other examples, unitary operators with $L^\dagger = L^{-1}$ and hermitian operators with $L^\dagger = L$ are normal. For any normal operator $L \in \mathrm{L}(\mathcal{H})$ there exists an orthonormal set $\{|e_i\rangle\}$ in $\mathcal{H}$ such that L can be written in *spectral decomposition*

$$L = \sum_i \lambda_i |e_i\rangle\langle e_i| \tag{2.24}$$

with the unique (up to ordering) *eigenvalues* $\lambda_i = \lambda_i(L) \in \mathbb{C}$ and *eigenvectors* $|e_i\rangle$. The set $\{|e_i\rangle\}$ of eigenvectors with nonzero eigenvalue forms an orthonormal basis of $\mathrm{supp}\, L = \mathrm{im}\, L$, and therefore the number of nonzero eigenvalues of L counted

with multiplicity is equal to rank L. The eigenbasis is unique if and only if all the eigenvalues are mutually different. Hermitian operators have real eigenvalues and the eigenvalues of positive operators are nonnegative, $\lambda_i \geq 0$. Given a positive operator $M \geq 0$, we define its unique positive square root as $\sqrt{M} := \sum_i \sqrt{\lambda_i}|e_i\rangle\langle e_i|$. Finally, the eigenvalues of unitary operators are *phases*, i.e., elements of the complex unit circle $\mathrm{U}(1) = \{\alpha \in \mathbb{C} : |\alpha| = 1\}$.

2.3.3 Singular Value Decomposition

For any general linear operator $L \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$, there exists a pair of orthonormal sets $\{|e_i\rangle \in \mathcal{H}\}$ and $\{|e'_i\rangle \in \mathcal{H}'\}$ such that L can be decomposed as

$$L = \sum_i s_i |e'_i\rangle\langle e_i|, \tag{2.25}$$

where the summation is over $i \in \{1, \ldots, \operatorname{rank} L\}$. This form is called *singular value decomposition* with the unique (up to ordering) positive numbers $s_i = s_i(L) > 0$, the *singular values*. The $s_i(L) = s_i(Q'LU)$ are invariant under unitaries $U \in \mathrm{L}(\mathcal{H})$ and $Q' \in \mathrm{L}(\mathcal{H}')$, as these can be absorbed into the orthonormal bases. The sets $\{|e_i\rangle\}$ and $\{|e'_i\rangle\}$ form orthonormal bases of the subspaces $\operatorname{supp} L$ and $\operatorname{im} L$, respectively. The operator $L^\dagger L = \sum_i s_i^2 |e_i\rangle\langle e_i| \in \mathrm{P}(\mathcal{H})$ is positive and consequently has a unique positive square root called the *modulus* of L,

$$|L| := \sqrt{L^\dagger L} = \sum_i s_i |e_i\rangle\langle e_i| \in \mathrm{P}(\mathcal{H}). \tag{2.26}$$

Therefore, the singular values $s_i(L)$ can be obtained by computing the eigenvalues $\lambda_i(|L|)$ of $|L|$. The singular value decomposition implies the following observation, which we employ frequently.

Lemma 2.1. *Let $M \in \mathrm{P}(\mathcal{H})$ be a positive operator written as $M = A^\dagger A$ with $A \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$. There is a partial isometry V such that $A = V\sqrt{M}$. If A is square, i.e., $A \in \mathrm{L}(\mathcal{H})$, V can be chosen unitary.*

Proof. Given the decompositions $M = \sum_i p_i |i\rangle\langle i|$ and $A = \sum_i s_i |e'_i\rangle\langle e_i|$, the assumption $M = A^\dagger A$ implies that $\sum_i p_i |i\rangle\langle i| = \sum_i s_i^2 |e_i\rangle\langle e_i|$. We conclude that $s_i = \sqrt{p_i}$ and $|i\rangle = |e_i\rangle$. Define the partial isometry $V|i\rangle = |e'_i\rangle$ which yields $A = V\sqrt{M}$. In the special case of a (square) operator $L \in \mathrm{L}(\mathcal{H})$, the partial isometry can be extended to a unitary U. For that, complete $\{|i\rangle\}$ and $\{|e'_i\rangle\}$ to orthonormal bases of $\mathcal{H}$, respectively. Then, the unitary is defined by $U|\tilde{e}_i\rangle = |\tilde{e}'_i\rangle$. □

A related result which directly follows from the singular value decomposition is the *polar decomposition* $L = V|L|$ of an operator $L \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$. By comparing Eqs. (2.25) and (2.26), we see that $V|e_i\rangle = |e'_i\rangle$ is a partial isometry from $\mathcal{H}$ to $\mathcal{H}'$ defined via the vectors appearing in the singular value decomposition of L.

CHAPTER 3

Quantum Mechanics

Quantum mechanics is the physical theory which describes nature at the scales and energy levels of atoms and subatomic particles. Despite more than one century of research, there are many open questions regarding the foundations of quantum mechanics. In particular, in the axiomatic formulation of quantum mechanics we employ, the postulates lack a physical or operational motivation. We introduce quantum mechanics from the viewpoint of information theory which focuses on concepts such as knowledge and uncertainty about a system. Therefore, we start with the *open* system formulation of quantum mechanics, in which states can be noisy and thus (the lack of) information can be described. Importantly, this allows us to describe classical information theory in the quantum language as classical random variables can be viewed as special quantum states. In the next chapter, we will see how one can get back to the *closed* system formulation, usually found in quantum mechanics textbooks, by enlarging the system under consideration.

We take an abstract approach by which a quantum experiment is necessarily composed of a *preparation* of a state and a *measurement* of it. If time elapses between the preparation event and measurement event, states and measurements can evolve in time. The necessity of this separation is one of the basic differences between quantum and classical physics, as in classical physics there is no need to introduce observables through measurements. Moreover, quantum mechanics is a *statistical* theory, meaning that it generally does not predict individual events, but only probabilities of outcomes in statistical experiments. As a consequence of recent experiments [GVW$^+$15, SMSC$^+$15, HBD$^+$15, Bed17], it is believed that this statistical character of quantum mechanics is not due to the incompleteness of the theory but rather a part of nature. This chapter is based on lecture notes [Ren13, Wol12, Wol14], Tomamichel's thesis [Tom12] and quantum information textbooks [NC00, Wil13].

3.1 Systems and States

The preparation of a quantum system is the set of actions which determines all probability distributions of any possible *measurement*. Since different preparations can result in equal probability distributions, the concept of a *state* is introduced

as the unique specification of the effect of a preparation. In the following, we use the words state and measurement to refer to both the physical concept and the mathematical operators.

Postulate 1 (States)**.** *A quantum system can be associated to a Hilbert space $\mathcal{H}$, such that any physical state of the system is uniquely described by a* density matrix*, that is, a positive operator $\rho \in \mathrm{P}(\mathcal{H})$ with unit trace,* $\mathrm{tr}(\rho) = 1$*. We denote the set of density matrices by* $\mathrm{S}(\mathcal{H})$*.*

We call (square) operators $L \in \mathrm{L}(\mathcal{H})$ *normalized* if $\mathrm{tr}(L) = 1$ and *subnormalized* if $0 < \mathrm{tr}(L) \leq 1$. We will often fix an orthonormal basis $\{|i\rangle\}$ of $\mathcal{H}$, called *computational basis*, in which we express density matrices. As a consequence of normalization, any density matrix can be parameterized by $d^2 - 1$ real parameters, where $d = \dim_{\mathbb{C}} \mathcal{H}$. It is important that density matrices can form a basis of the space of hermitian operators and the space of linear operators, i.e., $\mathrm{span}_{\mathbb{R}}(\mathrm{S}(\mathcal{H})) = \mathrm{H}(\mathcal{H})$ and $\mathrm{span}_{\mathbb{C}}(\mathrm{S}(\mathcal{H})) = \mathrm{L}(\mathcal{H})$. Such a basis is given by the set $\{\rho_{(i,j)} \in \mathrm{S}(\mathcal{H})\}$ defined as

$$\rho_{(i,j)} \coloneqq \begin{cases} \frac{1}{2}(|i\rangle + |j\rangle)(\langle i| + \langle j|) & \text{if } i < j \\ \frac{1}{2}(|i\rangle + i|j\rangle)(\langle i| - i\langle j|) & \text{if } i > j \\ |i\rangle\langle i| & \text{otherwise.} \end{cases} \tag{3.1}$$

3.1.1 Pure States

A *probability distribution* is a set $\{p_i\}$ of nonnegative real numbers $p_i \geq 0$ with $\sum_i p_i = 1$. Given a probability distribution $\{p_i\}$, the *convex combination* or *mixture* of a set $\{M_i \in \mathrm{H}(\mathcal{H})\}$ of hermitian operators is given by the hermitian operator $\sum_i p_i M_i$. The set of density matrices $\mathrm{S}(\mathcal{H})$ is a *convex set*, i.e., any convex combination of two (or more) states $\rho, \sigma \in \mathrm{S}(\mathcal{H})$ is also element of $\mathrm{S}(\mathcal{H})$.

Of particular importance are *pure* states that we define to be the states that lie on the boundary of the convex set $\mathrm{S}(\mathcal{H})$. Therefore, a pure state cannot be written as a convex combinations of states other than itself. Since quantum states $\rho \in \mathrm{S}(\mathcal{H})$ are hermitian, they can be written in spectral decomposition $\rho = \sum_i \lambda_i |i\rangle\langle i|$, where positivity and normalization imply that the eigenvalues λ_i form a probability distribution. Hence, we see that any pure state can have only one nonzero eigenvalue, because otherwise it could be written as the convex combination of different eigenstates. We conclude that pure states take the form $\rho = |\psi\rangle\langle\psi|$ with a normalized state vector $|\psi\rangle \in \mathcal{H}$ which is unique up to a phase factor $e^{i\phi} \in \mathrm{U}(1)$. We will often represent a pure state by its state vector. This implies that pure states are projectors $\rho^2 = \rho$, while the square of all other states, which we call *mixed*, is subnormalized, $\mathrm{tr}(\rho^2) < 1$. Moreover, pure states have rank one, while mixed states have rank larger than one.

The spectral decomposition $\rho = \sum_i p_i |i\rangle\langle i|$ of any mixed state can now be interpreted operationally. It describes a probabilisitic preparation of ρ, where the pure state $|i\rangle$ is prepared with probability p_i. In this sense, mixed states can be considered noisy, while pure states contain full information about a quantum system. In the next chapter, we will see that mixed states can be interpreted as states that contain correlations with the environment.

3.1.2 Composite Systems

The following postulate specifies how the Hilbert spaces of two systems can be combined to obtain the Hilbert space of the composite system.

Postulate 2 (Composition)**.** *The states of a joint system with component Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are described by the set of density matrices $\mathrm{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Moreover, if the states of the subsystems, ρ_A and ρ_B, are independent of each other, the state of the joint system is given by $\rho_A \otimes \rho_B$.*

For a quantum system composed of two subsystems, i.e., a *bipartite* system, we denote the subsystems by capital letters, e.g., A, B, and the joint density matrix by $\rho_{AB} \in \mathrm{S}(\mathcal{H}_{AB} \coloneqq \mathcal{H}_A \otimes \mathcal{H}_B)$. Whenever a linear operator $L_A \in \mathrm{L}(\mathcal{H}_A)$ is only defined on one subsystem, we extend its action on the whole space by $L_A \otimes \mathbb{1} \in \mathrm{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$. Therefore, $\mathrm{tr}(L_A \rho_{AB}) = \mathrm{tr}((L_A \otimes \mathbb{1}_B)\rho_{AB}) = \mathrm{tr}(L_A \,\mathrm{tr}_B(\rho_{AB}))$, where the last equality follows from property (2.18) of the partial trace. Since the state of system A is fully characterized by the action of all linear forms $\mathrm{tr}(L_A \cdot)$ on it, the system is fully described by $\mathrm{tr}_B(\rho_{AB})$. We call $\rho_A \coloneqq \mathrm{tr}_B(\rho_{AB})$ the *reduced state* on A, and $\rho_B \coloneqq \mathrm{tr}_A(\rho_{AB})$ the reduced state on B.

Entanglement

Bipartite quantum states ρ_{AB} can contain correlations in the sense that there exist local operators $L \in \mathrm{L}(\mathcal{H}_A)$ and $R \in \mathrm{L}(\mathcal{H}_B)$ such that

$$\mathrm{tr}(L \otimes R \rho_{AB}) \neq \mathrm{tr}(L\rho_A)\,\mathrm{tr}(R\rho_B). \tag{3.2}$$

However, these correlations can have a classical origin, i.e. arise due to a correlated preparation of states via a joint probability distribution. This motivates the definition of *classically correlated* or *separable* states, which are of the form

$$\rho_{AB} = \sum_i p_i \sigma_i \otimes \tau_i, \tag{3.3}$$

where $\sigma_i \in \mathrm{S}(\mathcal{H}_A)$, $\tau_i \in \mathrm{S}(\mathcal{H}_B)$ and $\{p_i\}$ is a probability distribution. The set of separable states is convex. Conversely, any state ρ_{AB} which cannot be written in the above form is said to be *entangled*. Entanglement is often perceived to embody

quantum correlations, which are a fundamental prerequisite for many quantum information protocols. In particular, in so-called nonlocal games [HHHH09, Bus12], entangled states can lead to correlations at the classical level that cannot be simulated by separable states.

The singular value decomposition implies an analogous decomposition of vectors on tensor spaces. This *Schmidt decomposition* of a vector is useful for the investigation of pure state entanglement.

Lemma 3.1 (Schmidt decomposition)**.** *For any vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ there exist orthonormal sets $\{|e_i\rangle \in \mathcal{H}_A\}$ and $\{|e'_i\rangle \in \mathcal{H}_B\}$ and unique positive numbers $\lambda_i > 0$ such that*

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}|e_i\rangle \otimes |e'_i\rangle, \quad \sum_i \lambda_i = \langle\psi|\psi\rangle, \tag{3.4}$$

where $d \leq \min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}$. The λ_i are called Schmidt coefficients and the number of (nonzero) λ_i is the Schmidt rank of $|\psi\rangle$. Moreover, a pure state $\rho = |\psi\rangle\langle\psi|$ is separable if and only if $|\psi\rangle$ has Schmidt rank of one.

Proof. Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be any vector in a tensor Hilbert space and let $\mathrm{vec}_{\mathcal{B}}$ be the isomorphism defined in Eq. (2.20). For any basis $\mathcal{B}$ of $\mathcal{H}_A \otimes \mathcal{H}_B$, $L := \mathrm{vec}_{\mathcal{B}}^{-1}(|\psi\rangle)$ is an operator in $\mathrm{L}(\mathcal{H}_B, \mathcal{H}_A)$. Now, we fix $\mathcal{B} = \{|e_i\rangle \otimes |e'_j\rangle\}$ to be the basis such that $L = \sum_i s_i |e_i\rangle\langle e'_i|$ is in its singular value form (2.25). This implies

$$|\psi\rangle = \mathrm{vec}_{\mathcal{B}}(L) = \mathrm{vec}_{\mathcal{B}}\Big(\sum_i s_i |e_i\rangle\langle e'_i|\Big) = \sum_i s_i |e_i\rangle \otimes |e'_i\rangle, \tag{3.5}$$

which is the Schmidt decomposition of $|\psi\rangle$ if we write $s_i = \sqrt{\lambda_i}$, i.e., the Schmidt coefficients of $|\psi\rangle$ are the squares of the singular values of $\mathrm{vec}_{\mathcal{B}}^{-1}(|\psi\rangle)$.

For the second assertion, suppose that ρ is pure and separable $\rho = \sum_i p_i \sigma_i \otimes \tau_i$. Because ρ is rank one, every (normalized) product term $\sigma_i \otimes \tau_i$ must be equal to ρ. Therefore $\rho = |\psi\rangle\langle\psi| = |e\rangle\langle e| \otimes |f\rangle\langle f|$, i.e., $|\psi\rangle = |e\rangle \otimes |f\rangle$ has Schmidt rank of one. □

The Schmidt decomposition can be computed efficiently without making use of the singular value decomposition. Consider the reduced states $\rho_A = \mathrm{tr}_B(|\psi\rangle\langle\psi|)$ and $\rho_B = \mathrm{tr}_A(|\psi\rangle\langle\psi|)$: the vectors $|e_i\rangle \in \mathcal{H}_A$ ($|e'_i\rangle \in \mathcal{H}_B$) from Lemma 3.1 are the eigenvectors with nonzero eigenvalue of ρ_A (ρ_B). The Schmidt coefficients are the corresponding eigenvalues $\lambda_i = \lambda_i(\rho_A)$. In particular, the existence of the Schmidt decomposition implies that the reduced density matrices of a pure state have the same nonzero eigenvalues.

A pure state is called *maximally entangled* if it has Schmidt coefficients $\lambda_i = \frac{1}{d}$, where $d = \min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}$. We call the following vector the *canonical*

maximally entangled state

$$|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle, \quad |\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \tag{3.6}$$

which is in Schmidt decomposition form (3.4) with respect to the computational basis $\{|i\rangle\}$.

Lemma 3.2 (Maximally entangled states)**.** *Let $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle \in \mathcal{H} \otimes \mathcal{H}$ be a maximally entangled state. For any operator $L \in \mathrm{L}(\mathcal{H})$ it holds that*

$$(L \otimes \mathbb{1})|\Psi\rangle = (\mathbb{1} \otimes L^T)|\Psi\rangle, \tag{3.7}$$

where the transposition is taken with respect to the Schmidt basis of $|\Psi\rangle$. Consequently, for any bipartite pure state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ with reduced density matrix ρ_A there exists a unitary U such that it can be written as

$$|\psi\rangle = (K \otimes \mathbb{1})|\Psi\rangle, \quad K \coloneqq \sqrt{d}\sqrt{\rho}_A U. \tag{3.8}$$

Proof. For the first assertion, we expand L in the computational basis $L = \sum_{j,k} L_{j,k} |j\rangle\langle k|$, such that $L|i\rangle = \sum_j L_{j,i}|j\rangle$. Therefore,

$$\begin{aligned}(L \otimes \mathbb{1})|\Psi\rangle &= \frac{1}{\sqrt{d}} \sum_{i,j} L_{j,i} |j\rangle \otimes |i\rangle = \frac{1}{\sqrt{d}} \sum_j |j\rangle \otimes \sum_i L^T_{i,j} |i\rangle \\ &= \frac{1}{\sqrt{d}} \sum_j |j\rangle \otimes L^T |j\rangle = (\mathbb{1} \otimes L^T)|\Psi\rangle. \end{aligned} \tag{3.9}$$

For the second assertion, let $|\psi\rangle = \sum_i \sqrt{\lambda_i}|e_i\rangle \otimes |e'_i\rangle$ be in Schmidt form such that $\rho_A = \sum_j \lambda_j |e_j\rangle\langle e_j|$. Let Q, V be unitaries such that $Q|i\rangle = |e_i\rangle$ and $V^T|i\rangle = |e'_i\rangle$ and define $U \coloneqq QV$ which is unitary as well. Therefore,

$$\begin{aligned}(K \otimes \mathbb{1})|\Psi\rangle &= (\sqrt{d}\sqrt{\rho}_A U \otimes \mathbb{1})|\Psi\rangle = (\sqrt{d}\sqrt{\rho}_A Q \otimes \mathbb{1})(V \otimes \mathbb{1})|\Psi\rangle \\ &= (\sqrt{d}\sqrt{\rho}_A Q \otimes \mathbb{1})(\mathbb{1} \otimes V^T)|\Psi\rangle = \sum_i \sqrt{\rho}_A Q|i\rangle \otimes V^T|i\rangle \\ &= \sum_{i,j} \sqrt{\lambda_j}|e_j\rangle\langle e_j|e_i\rangle \otimes |e'_i\rangle = \sum_i \sqrt{\lambda_i}|e_i\rangle \otimes |e'_i\rangle = |\psi\rangle. \end{aligned} \tag{3.10}$$

□

3.1.3 Classical Systems

Quantum information theory can be considered as a generalization of classical information theory. This is because the constituents of classical information theory, *random variables*, are describable in the quantum formalism. For the purpose of this

thesis, a random variable is a set $X = \{x \in \mathcal{X}\}$, where $\mathcal{X} \subset \mathbb{R}$ is discrete and called *alphabet*, such that each element x is associated to a probability p_x. The probability distribution $\{p_x\}$ is also called the state of the random variable X. Let $\{|x\rangle\}_{x\in\mathcal{X}}$ be the computational basis of a Hilbert space $\mathcal{H}_X$ such that $\dim \mathcal{H}_X = |\mathcal{X}|$. Then, the state of the random variable X is represented by the quantum state

$$\rho_X = \sum_{x\in\mathcal{X}} p_x |x\rangle\langle x|, \tag{3.11}$$

which is a positive normalized operator because $\{p_x\}$ is a probability distribution. We call a quantum system X with only states of the above form a *classical* system. In the following, we will see that classical systems can be used to describe the outcomes of measurements.

We can also consider composite systems where one or more subsystems are classical. Let X be a classical system and A be a quantum system. Then, a joint state $\rho_{XA} \in \mathrm{S}(\mathcal{H}_X \otimes \mathcal{H}_A)$, is called *classical-quantum* state (CQ-state) and takes the form

$$\rho_{XA} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x, \tag{3.12}$$

where $\{p_x\}$ is a probability distribution and $\rho_x \in \mathrm{S}(\mathcal{H}_A)$. These states are of the form (3.3) and, thus, are separable. A special case is the state of two classical systems X and Y which takes the form

$$\begin{aligned}\rho_{XY} &= \sum_{x,y} p_{x,y} |x\rangle\langle x| \otimes |y\rangle\langle y| \\ &= \sum_x p_x |x\rangle\langle x| \otimes \sum_y p(y|x) |y\rangle\langle y|,\end{aligned} \tag{3.13}$$

where the probability distribution $\{p_x := \sum_y p_{x,y}\}$ is called *marginal* of $\{p_{x,y}\}$, and $\{p(y|x) := \frac{p_{x,y}}{p_x}\}$ is called *conditional* probability distribution on Y. Marginal probabilities are compatible with reduced states in the sense that $\rho_X = \mathrm{tr}_Y(\rho_{XY})$ is the quantum state that represents the marginal $\{p_x\}$.

3.2 Measurements and Observables

Information about a quantum system can only be obtained by performing a measurement in a statistical experiment. The fundamental abstract notion of a (general) *quantum measurement* provides the basis for all observables, i.e., physical properties of a quantum system. In contrast to classical physics, a quantum measurement generally disturbes the measured state, even on average.

Postulate 3. *A measurement on a quantum system with Hilbert space $\mathcal{H}$ is described by a set $\boldsymbol{E} = \{E_i\}$ of positive operators $E_i \geq 0$ on $\mathcal{H}$, satisfying the completeness relation $\sum_i E_i = \mathbb{1}$. If $\boldsymbol{E}$ is measured on the state $\rho \in \mathrm{S}(\mathcal{H})$, the probability of observing the outcome i is given by $p_i = \mathrm{tr}(E_i\rho)$.*

A quantum measurement $\boldsymbol{E}$ is also called a positive-operator-valued measure (POVM), and its elements are called *effects*. An n-outcome POVM has $n \in \mathbb{N}$ effects. We call a POVM *informationally complete* if its effects form a basis of the space of hermitian operators $\mathrm{H}(\mathcal{H})$. Therefore, a quantum state ρ is uniquely characterized by the outcome probabilities $p_i = \mathrm{tr}(E_i\rho)$ of an informationally complete POVM. A projective measurement $\boldsymbol{P} = \{P_i\}$ is a POVM whose effects form a projector family, i.e., $P_iP_j = \delta_{i,j}P_j$. The standard example of a projective measurement is the measurement $\boldsymbol{P} = \{|i\rangle\langle i|\}$ in the computational basis $\{|i\rangle\}$.

3.2.1 Extremal Measurements

A POVM is called *linearly independent* if its effects are linearly independent, and it is called *rank one*, if its effects have rank one. In order to define mixtures of POVMs, it is useful to write the n-outcome POVM $\boldsymbol{E} = \{E_i\}$ as the n-tuple of operators $\boldsymbol{E} = (E_1, \ldots, E_n)$. Then, the multiplication with a scalar α and the addition of two n-outcome POVMs $\boldsymbol{E}, \boldsymbol{F}$ on the same Hilbert space is defined element-wise

$$\begin{aligned} \boldsymbol{E} + \boldsymbol{F} &\coloneqq (E_1 + F_1, \ldots, E_n + F_n), \\ \alpha\boldsymbol{E} &\coloneqq (\alpha E_1, \ldots, \alpha E_n), \quad \alpha \in \mathbb{C}. \end{aligned} \tag{3.14}$$

For any probability $p \in [0, 1]$, the mixture or convex combination of two POVMs $\boldsymbol{E}, \boldsymbol{F}$ is defined as $p\boldsymbol{E} + (1-p)\boldsymbol{F}$, which is also a POVM [OGWA17]. Therefore, given a Hilbert space $\mathcal{H}$, the set of quantum measurements on it is a convex set. Measurements on the boundary of this set are called *extremal* [DPP05]. Thus, extremal measurements cannot be expressed by a (nontrivial, i.e., $p \in (0, 1)$) convex combination of two different POVMs. Any general POVM can be obtained from extremal (rank-one) POVMs by mixing and relabeling [HHP12]. Relabeling, also called coarse-graining, is the procedure where the labels of the POVM effects are shuffled and combined, where the latter means that a single label is given to the sum of effects. The fact that classical post-processing of extremal measurements leads to the most general POVM makes extremal measurement the analog of pure quantum states. However, extremal measurements are harder to characterize. Any linearly-independent rank-one POVM is extremal, which in particular includes rank-one projective measurements. Moreover, the most general extremal measurement can be obtained from an extremal rank-one POVM by relabeling [HHP12].

3.2.2 Observables and Measurement Process

Physical properties of a quantum system are represented by *observables*, which we introduce via quantum measurements. More precisely, any physical property of a quantum system is represented by an observable and the value of the property is (only) revealed by an underlying measurement. In contrast to classical physics, quantum mechanics does not describe the physical properties of a system before a measurement.

Definition 3.1. *An observable $\boldsymbol{N}$ is a POVM $\{N_i\}$, where each effect N_i is associated to a real number $n_i \in \mathbb{R}$, the measurement outcome. Given a quantum system in state ρ, the expectation value of the observable is given by*

$$\langle \boldsymbol{N} \rangle \coloneqq \sum_i p_i n_i, \quad p_i = \mathrm{tr}(N_i \rho). \tag{3.15}$$

We associate to any observable the hermitian operator $M \coloneqq \sum_i n_i N_i \in \mathrm{H}(\mathcal{H})$, such that the expectation value of the observable can be expressed as $\langle \boldsymbol{N} \rangle = \langle M \rangle = \mathrm{tr}(M\rho)$. The spectral theorem implies that if $\boldsymbol{N}$ is projective, the observable is fully described by M: the measurement outcomes n_i are the eigenvalues of M and the POVM effects N_i are the corresponding projectors on the eigenspace.

Performing a measurement (partially) characterizes the measured quantum state, but the state after the measurement with outcome i is not uniquely specified. This is why we introduce the notion of *measurement process* to eliminate this ambiguity. It turns out that any operator A_i with $E_i = A_i^\dagger A_i$ defines a *compatible* (possible) post-measurement state as follows. The subnormalized state $\hat{\rho}_i' = A_i \rho A_i^\dagger$ is positive and leads to the right outcome probability $\mathrm{tr}(A_i \rho A_i^\dagger) = \mathrm{tr}(E_i \rho)$ for any state ρ.

Definition 3.2 (Measurement process)**.** *A measurement process is a POVM $\boldsymbol{E} = \{E_i\}$ on $\mathcal{H}$ together with the specification of compatible post-measurement states ρ_i'. It can be described by a collection of operators $\boldsymbol{A} = \{A_i\}$ with $A_i \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ such that $E_i = A_i^\dagger A_i$ and $\rho_i' = \frac{1}{p_i} A_i \rho A_i^\dagger$, and where $p_i = \mathrm{tr}(E_i \rho)$.*

We call $\boldsymbol{A}$ a set of *measurement operators* for the POVM $\boldsymbol{E}$. As a consequence of Lemma 2.1, any measurement operator compatible with E_i is given by $A_i = V_i \sqrt{E_i}$, where $V_i \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ is a partial isometry. For a projective measurement $\boldsymbol{P}$, each effect is also a measurement operator, $P_i = P_i^\dagger P_i$. Thus, for projective measurements we always employ the set $\{P_i\}$ as measurement operators. A *non-selective* measurement process is the map $\mathcal{A}[\rho] = \sum_i p_i \rho_i' = \sum_i A_i \rho A_i^\dagger$, which corresponds to the average state after the measurement, i.e., when the information about the outcome is lost. In the next section we study such processes from the (seemingly) broader perspective of time evolutions.

3.3 Evolution of States and Measurements

In the quantum formalism, preparations and measurements are described by density operators and POVMs, respectively. If time elapses between the preparation and measurement event, both parts can evolve in time. It is convenient to either fully associate the time evolution to states, which is called *Schrödinger picture*, or fully to POVMs, which is called *Heisenberg picture*. In the following, we will mostly focus on the Schrödinger picure and occasionally comment on the Heisenberg picture. A quantum state evolves in time through the action of a *quantum channel*, which is the most general transformation mapping density matrices to density matrices in a consistent way. In particular, quantum channels need to be linear to be consistent with the probabilistic interpretation of convex combinations. This is why we introduce the concept of superoperators.

3.3.1 Superoperators

Given two Hilbert spaces $\mathcal{H}, \mathcal{H}'$, a *superoperator* $\mathcal{E}\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ is a linear map between the respective operator spaces. In the case $\mathcal{H}' = \mathcal{H}$, we simply call $\mathcal{E}$ a superoperator on $\mathrm{L}(\mathcal{H})$. We denote the identity superoperator on $\mathrm{L}(\mathcal{H})$ by id. The set of superoperators is a vector space and the tensor product of superoperators is defined in analogy to Eq. (2.12).

The *composition* of any two superoperators $\mathcal{E}, \mathcal{L}$ is defined as the superoperator $(\mathcal{E} \circ \mathcal{L})[\cdot] \coloneqq \mathcal{E}[\mathcal{L}[\cdot]]$. For any superoperator $\mathcal{E}\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ its adjoint superoperator $\mathcal{E}^\dagger\colon \mathrm{L}(\mathcal{H}') \to \mathrm{L}(\mathcal{H})$ is defined via the Hilbert-Schmidt scalar product (2.19) as the unique operator satisfying

$$\langle L, \mathcal{E}[R]\rangle = \langle \mathcal{E}^\dagger[L], R\rangle \tag{3.16}$$

for all $L \in \mathrm{L}(\mathcal{H}')$ and $R \in \mathrm{L}(\mathcal{H})$.

Definition 3.3. *A superoperator* $\mathcal{E}\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ *is called a* positive map *if* $\mathcal{E}[M] \geq 0$ *holds for any* $M \geq 0$.

However, for quantum mechanics a stronger condition is needed. *Completely positive maps* have the property that when they are applied to only a subsystem of a joint (entangled) quantum system, the state after the map remains positive.

Definition 3.4. *A superoperator* $\mathcal{E}\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ *is completely positive (CP) if for any operator space* $\mathrm{L}(\mathcal{H}_R)$ *of arbitrary dimension,* $\mathcal{E} \otimes \mathrm{id}_R$ *is a positive map.*

An important example of a completely positive map is obtained from a set of operators $\{K_i \in \mathrm{L}(\mathcal{H}, \mathcal{H}')\}$, defining the map $\mathcal{E}[L] = \sum_i K_i L K_i^\dagger$, for $L \in \mathrm{L}(\mathcal{H})$.

This map is CP because with $|\psi_i\rangle = (K_i \otimes \mathbb{1})^\dagger |\psi'\rangle$ and $M \in \mathrm{P}(\mathcal{H} \otimes \mathcal{H}_R)$, it holds that

$$\begin{aligned}\langle\psi'|\mathcal{E} \otimes \mathrm{id}_R[M]|\psi'\rangle &= \sum_i \langle\psi'|(K_i \otimes \mathbb{1})M(K_i \otimes \mathbb{1})^\dagger|\psi'\rangle \\ &= \sum_i \langle\psi_i|M|\psi_i\rangle \geq 0 \quad \text{if } M \geq 0,\end{aligned} \tag{3.17}$$

We later show in Theorem 3.4 that, remarkably, every CP map can be written in the above form.

3.3.2 Channels

A superoperator $\mathcal{E}$ is *trace-preserving* (TP) if $\mathrm{tr}(\mathcal{E}[L]) = \mathrm{tr}(L)$ for all $L \in \mathrm{L}(\mathcal{H})$ and it is *trace-nonincreasing* (TN) if $\mathrm{tr}(\mathcal{E}[L]) \leq \mathrm{tr}(L)$. We call any completely positive map CPTP if it is trace-preserving, and CPTN if it is trace-nonincreasing. Moreover, we call a superoperator $\mathcal{E}$ *unital* if it satisfies $\mathcal{E}[\mathbb{1}] = \mathbb{1}$. For any CPTP map $\mathcal{E}$ its adjoint superoperator $\mathcal{E}^\dagger$ is completely positive and unital, where unitality follows from

$$\mathrm{tr}(\mathcal{E}^\dagger[\mathbb{1}]L) = \mathrm{tr}(\mathcal{E}[L]) = \mathrm{tr}(L) \tag{3.18}$$

for any $L \in \mathrm{L}(\mathcal{H})$.

Postulate 4. *The time evolution of quantum states $\rho \in \mathrm{S}(\mathcal{H})$ is described by quantum channels Λ, which are completely positive trace-preserving (CPTP) maps on $\mathrm{L}(\mathcal{H})$.*

In contrast, in the Heisenberg picture of quantum mechanics, POVMs evolve via completely positive unital maps. In particular, for any quantum channel Λ in the Schrödinger picture, $\Lambda^\dagger$ is a quantum channel in the Heisenberg picture. If the input and output spaces match, compositions and also convex combinations of quantum channels are again quantum channels. We note that the partial trace operation is a channel. Given an isometry $V \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$, we define the corresponding *isometric channel* as $\mathcal{V}[\rho] = V\rho V^\dagger$. Likewise, a unitary $U \in \mathrm{L}(\mathcal{H})$ defines the *unitary channel* $\mathcal{U}[\rho] = U\rho U^\dagger$. Only unitary channels have the property that the inverse map $\mathcal{U}^{-1}$ is also a (unitary) channel, i.e., the evolution is reversible. Therefore, unitary channels corresponds to a noise-free evolution as no information is lost.

Deciding whether a superoperator $\mathcal{E}$ is completely positive seems a priori to involve an infinite number of conditions, namely for any dimension of $\mathcal{H}_R$ in (3.4). The following theorem establishes a duality between quantum channels and bipartite quantum states, and thereby simplifies the check of completely positivity.

Theorem 3.3 (Choi theorem)**.** *Let $\mathcal{H}_R \simeq \mathcal{H}$ be isomorphic Hilbert spaces with the maximally entangled state $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle_R \otimes |i\rangle \in \mathcal{H}_R \otimes \mathcal{H}$. Given a superoperator $\mathcal{E} : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$, the following map is an isomorphism*

$$\mathcal{E} \mapsto J_\mathcal{E} \coloneqq \mathcal{E} \otimes \mathrm{id}[|\Psi\rangle\langle\Psi|] \quad \in \mathrm{L}(\mathcal{H}' \otimes \mathcal{H}). \tag{3.19}$$

Its inverse maps a bipartite operator $J \in \mathrm{L}(\mathcal{H}' \otimes \mathcal{H})$ to the superoperator

$$\mathcal{E}_J[L] = d \, \mathrm{tr}_\mathcal{H}(J(\mathbb{1} \otimes L^T)) \quad \textit{from } \mathrm{L}(\mathcal{H}) \textit{ to } \mathrm{L}(\mathcal{H}'), \tag{3.20}$$

where L^T denotes the transposition with respect to $\{|i\rangle\}$, and $d = \dim \mathcal{H}$. Moreover, the following equivalences hold:

- *$\mathcal{E}$ preserves hermiticity, $\mathcal{E}[M]^\dagger = \mathcal{E}[M]$ $\forall M \in \mathrm{H}(\mathcal{H})$, iff $(J_\mathcal{E})^\dagger = J_\mathcal{E}$*
- *$\mathcal{E}$ is completely positive if and only if $J_\mathcal{E} \geq 0$*
- *$\mathcal{E}$ is trace-preserving if and only if $\mathrm{tr}_{\mathcal{H}'}(J_\mathcal{E}) = \frac{\mathbb{1}}{d}$*
- *$\mathcal{E}$ is unital if and only if $\mathrm{tr}_\mathcal{H}(J_\mathcal{E}) = \frac{\mathbb{1}}{d'}$, where $d' = \dim \mathcal{H}'$*

A proof of this theorem can be found, e.g., in [Wil13]. Remarkably, the Choi theorem tells us that in order to check whether a superoperator $\mathcal{E}$ is completely positive, one needs to check just one condition, namely whether the *Choi matrix* $J_\mathcal{E}$ is positive. In particular, $\mathcal{E}$ is a quantum channel (CPTP) if and only if $J_\mathcal{E}$ is a quantum state. As an application of the theorem above we prove the extremely useful *Kraus decomposition*, or operator-sum representation.

Theorem 3.4 (Kraus decomposition)**.** *A superoperator $\mathcal{E} : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ is completely positive if and only if it can be written as*

$$\mathcal{E}[L] = \sum_{i=1}^{r} K_i L K_i^\dagger, \tag{3.21}$$

with the Kraus operators $K_i \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$. Moreover, the following assertions hold:

- *The minimal number of Kraus operators is called the Choi rank of $\mathcal{E}$ and given by $r_{\min} = \mathrm{rank}(J_\mathcal{E}) \leq \dim \mathcal{H} \cdot \dim \mathcal{H}'$*
- *$\mathcal{E}$ is trace-preserving iff $\sum_i K_i^\dagger K_i = \mathbb{1}$, and $\mathcal{E}$ is unital iff $\sum_i K_i K_i^\dagger = \mathbb{1}$*
- *The adjoint superoperator admits the form $\mathcal{E}^\dagger[L] = \sum_{i=1}^r K_i^\dagger L K_i$*

Proof. According to Theorem 3.3 a superoperator $\mathcal{E}$ is completely positive if and only if its Choi matrix $J_\mathcal{E}$ is positive. By the spectral theorem, $J_\mathcal{E} \in \mathrm{L}(\mathcal{H}' \otimes \mathcal{H})$ can be decomposed into positive rank one operators

$$J_\mathcal{E} = \sum_{i=1}^{r} |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{r} (K_i \otimes \mathbb{1})|\Psi\rangle\langle\Psi|(K_i \otimes \mathbb{1})^\dagger, \tag{3.22}$$

where in the second equality we have used Lemma 3.2 with the maximally entangled state $|\Psi\rangle$. Comparing the right side of (3.22) with the definition of the Choi matrix $J_\mathcal{E} = \mathcal{E}\otimes\mathrm{id}(|\Psi\rangle\langle\Psi|)$ leads to the desired operator-sum decomposition (3.21), because of the one-to-one correspondence of a superoperator and its Choi matrix. This argument also shows that $r \geq \mathrm{rank}(J_\mathcal{E})$ and equality $r_{\min} = \mathrm{rank}(J_\mathcal{E})$ can be achieved if the $|\psi_i\rangle$ are chosen to be linearly independent.

Conversely, Eq. (3.22) also implies that any superoperator which can be written as $\mathcal{E}[L] = \sum_i K_i L K_i^\dagger$ leads to a positive Choi matrix $J_\mathcal{E} \geq 0$ and therefore, $\mathcal{E}$ is a CP map which we have already verified directly in (3.17). With the decomposition (3.21), it is clear that $\mathcal{E}$ is unital iff $\sum_i K_i K_i^\dagger = \mathbb{1}$. The condition for trace-preservation, $\sum_i K_i^\dagger K_i = \mathbb{1}$, directly follows from

$$\mathrm{tr}(\mathcal{E}[L]) = \mathrm{tr}(\sum_i K_i L K_i^\dagger) = \mathrm{tr}(\sum_i K_i^\dagger K_i L). \tag{3.23}$$

Finally, the Kraus decomposition of the adjoint superoperator follows from

$$\begin{aligned}\langle L, \mathcal{E}[R]\rangle &= \mathrm{tr}(L^\dagger \mathcal{E}[R]) = \mathrm{tr}(L^\dagger \sum_i K_i R K_i^\dagger) \\ &= \mathrm{tr}((\sum_i K_i^\dagger L K_i)^\dagger R) = \langle \mathcal{E}^\dagger[L], R\rangle,\end{aligned} \tag{3.24}$$

where we have used the definition of the adjoint superoperator with respect to the Hilbert-Schmidt scalar product. □

The Kraus decomposition implies that a measurement process (3.2), remarkably, is already the most general time evolution of a quantum state.

3.3.3 Qubit Bloch Representation

A quantum two-level system is called a *qubit* and it is described by a two-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$. Qubits are the simplest quantum systems and, similar to classical bits, are often used as building blocks of larger quantum systems. The qubit *Pauli matrices* are defined as

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.25}$$

and are also called Pauli-X, Pauli-Y, and Pauli-Z matrix, respectively. The Pauli matrices are unitary, hermitian, traceless ($\mathrm{tr}(\sigma_i) = 0$) and satisfy the relation

$$\sigma_i \sigma_j = \delta_{i,j} \mathbb{1} + i \sum_k \epsilon_{i,j,k} \sigma_k, \tag{3.26}$$

with the (totally anti-symmetric) Levi-Civita symbol $\epsilon_{i,j,k}$. Together with the qubit identity $\mathbb{1}$ the Pauli matrices form a Hilbert-Schmidt orthogonal basis of the space of hermitian operators $\mathrm{H}(\mathbb{C}^2)$. Consequently, qubit hermitian matrices can be expressed conveniently in the *Bloch sphere* representation. Any hermitian operator $M \in \mathrm{H}(\mathbb{C}^2)$ is in one-to-one relation with the pair $(\alpha, \vec{r})$, where $\alpha \in \mathbb{R}$ and the *Bloch vector* $\vec{r} = (r_1, r_2, r_3) \in \mathbb{R}^3$ is defined by

$$M = \alpha(\mathbb{1} + \vec{r} \cdot \vec{\sigma}), \quad r_i = \frac{\mathrm{tr}(\sigma_i M)}{2\alpha}, \tag{3.27}$$

with the vector of Pauli matries $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$, and $\vec{r} \cdot \vec{\sigma} = \sum_i r_i \sigma_i$. In particular, the operator M is a density matrix ρ if and only if $\alpha = \frac{1}{2}$ and $|\vec{r}| \leq 1$, ensuring normalization and positivity, respectively. Therefore, any qubit density matrix can be represented by a vector in the unit ball of $\mathbb{R}^3$. Moreover, pure states lie on the boundary of the sphere, i.e., $\rho^2 = \rho$ is equivalent to $|\vec{r}| = 1$.

The Bloch sphere representation is useful to visualize qubit POVMs. Any qubit POVM $\boldsymbol{E} = \{E_i\}$ can be decomposed as

$$\begin{gathered} E_i = \alpha_i(\mathbb{1} + \vec{m}_i \cdot \vec{\sigma}) \quad \text{with} \\ \alpha_i \geq 0, \quad |\vec{r}_i| \leq 1, \quad \sum_i \alpha_i = 1, \quad \sum_i \alpha_i \vec{r}_i = 0. \end{gathered} \tag{3.28}$$

As an example, we consider the qubit trine POVM

$$\boldsymbol{E}^{\mathrm{trine}} = \{\frac{2}{3}|\phi_k\rangle\langle\phi_k|\}_{k=1}^3, \tag{3.29}$$

with measurement vectors $|\phi_k\rangle$ given by

$$|\phi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega^{k-1}|1\rangle), \quad \text{where } \omega = e^{\frac{2\pi i}{3}}. \tag{3.30}$$

The trine POVM is extremal and can be considered as the simplest example of a symmetric extremal nonprojective POVM. We will utilize this measurement in Chapter 7 in the context of the resource theory of POVM-based coherence. In Fig. 3.1 below, we show the Bloch sphere, as well as the the Bloch vectors (measurement directions) $\vec{m}_k$ of the effects E_k^{trine}.

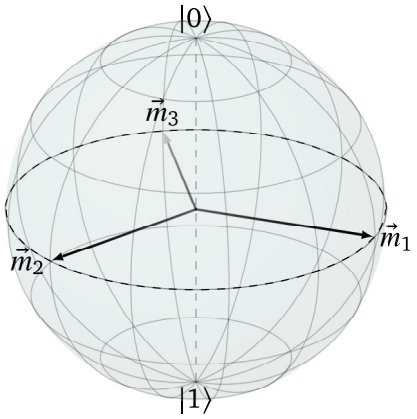

Figure 3.1: Bloch sphere representation of subnormalized positive qubit operators. The computational basis states $|0\rangle, |1\rangle$ lie on the z-axis. The vectors $\vec{m}_k$ indicate the measurement directions of the qubit trine POVM in the xy-plane, which is given in Eq. (3.29).

CHAPTER 4

Purified Quantum Mechanics

In the previous chapter, we introduced quantum mechanics from the open system viewpoint, in which partial information in terms of noisy state preparations, noisy measurements and classical random variables could be embedded in the description. In this chapter, we describe a process called *purification* which tells us that the lack of information about a quantum system can be thought of as arising from quantum correlations with an environment that we did not include in the description. This exclusion of correlated degrees of freedom necessarily leads to an incomplete local description and thus results in noise. Once we take the purifying system, i.e., any system that interacts with the one under consideration, into account, the noisy quantum system can be viewed as part of a larger noiseless global system. In the closed global system, quantum physics is described in terms of the traditional quantum formalism from textbooks, i.e., states are pure, measurements are projective, and evolutions are unitary. This chapter is based on the resources [Wil13, Wol12].

4.1 State Purification

Every mixed state on a finite-dimensional Hilbert space can be viewed as the reduced state of a bipartite pure state, called purification.

Definition 4.1 (Purification)**.** *A purification of a density matrix $\rho \in \mathrm{S}(\mathcal{H})$ is a pure bipartite state $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}_R$ such that its reduced state is equal to ρ*

$$\rho = \mathrm{tr}_R(|\psi\rangle\langle\psi|). \tag{4.1}$$

Theorem 4.1 (Purification)**.** *For every density matrix $\rho \in \mathrm{S}(\mathcal{H})$ there exists a purification $|\psi\rangle \in \mathcal{H}\otimes\mathcal{H}_R$. The minimal dilation space $\mathcal{H}_R^{\min}$ has $\dim(\mathcal{H}_R^{\min}) = \mathrm{rank}\,\rho$. If $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}_R^{\min}$ is a purification of ρ then all other purifications are of the form $|\psi'\rangle = (\mathbb{1} \otimes V)|\psi\rangle$, where $V \in \mathrm{L}(\mathcal{H}_R^{\min}, \mathcal{H}_R)$ is an isometry.*

Proof. Let $\rho = \sum_i p_i |i\rangle\langle i|$ be in spectral decomposition. For any orthonormal set $\{|e_i\rangle \in \mathcal{H}_R\}_{i=1}^r$ of size $r = \mathrm{rank}\,\rho$, the pure state $|\psi\rangle = \sum_i \sqrt{p_i}|i\rangle \otimes |e_i\rangle$ is a purification of ρ, since

$$\mathrm{tr}_R(|\psi\rangle\langle\psi|) = \sum_{i,j} \sqrt{p_i p_j}|i\rangle\langle j|\langle e_j|e_i\rangle = \rho. \tag{4.2}$$

Conversely, any pure state $|\psi\rangle \in \mathcal{H}\otimes\mathcal{H}_R$ which is not of the form $|\psi\rangle = \sum_i \sqrt{p_i}|i\rangle\otimes|e_i\rangle$ cannot be a purification of ρ. Therefore the minimal dimension of $\mathcal{H}_R$ is $\dim(\mathcal{H}_R^{\min}) = \operatorname{rank}\rho$.

Let $|\psi\rangle = \sum_i \sqrt{p_i}|i\rangle\otimes|e_i\rangle \in \mathcal{H}\otimes\mathcal{H}_R^{\min}$ and $|\psi'\rangle = \sum_i \sqrt{p_i}|i\rangle\otimes|e_i'\rangle \in \mathcal{H}\otimes\mathcal{H}_R$ be two purifications of ρ, where $|e_i'\rangle$ is an orthonormal set in $\mathcal{H}_R$. Define $V|e_i\rangle = |e_i'\rangle$ which is an isometry such that $|\psi'\rangle = (\mathbb{1}\otimes V)|\psi\rangle$. □

The *canonical purification* of ρ is the state $|\psi\rangle = (\sqrt{d\rho}\otimes\mathbb{1})|\Psi\rangle$, where $|\Psi\rangle$ denotes the canonical maximally entangled state (3.6). In this case, for $\rho = \sum_i p_i|i\rangle\langle i|$, the purifying system is equipped with the computational basis $\{|i\rangle\}$,

$$|\psi\rangle = (\sqrt{d\rho}\otimes\mathbb{1})|\Psi\rangle = \sum_{i,j}\sqrt{p_i}|i\rangle\langle i|j\rangle\otimes|j\rangle = \sum_i \sqrt{p_i}|i\rangle\otimes|i\rangle. \tag{4.3}$$

The purification of a quantum state has many applications in quantum information theory. It is of particular importance for quantum cryptography and randomness generation. Also, it can be used to obtain a relation between any two convex decompositions of a density matrix.

Lemma 4.2 (Relation between convex decompositions)**.** *Let ρ be a density matrix admitting the two convex decompositions,*

$$\rho = \sum_{i=1}^{d} p_i|\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{d'} q_i|\phi_i\rangle\langle\phi_i|, \tag{4.4}$$

where $d \le d'$ and $|\psi_i\rangle, |\phi_i\rangle$ are pure states. There exists an isometry V such that

$$\sqrt{q_i}|\phi_i\rangle = \sum_j V_{i,j}\sqrt{p_j}|\psi_j\rangle. \tag{4.5}$$

Proof. Let $|\psi\rangle = \sum_j \sqrt{p_j}|\psi_j\rangle\otimes|j\rangle$ and $|\phi\rangle = \sum_i \sqrt{q_i}|\phi_i\rangle\otimes|i\rangle$ be two purifications of ρ. According to Theorem 4.1 there exists an isometry V such that $|\phi\rangle = (\mathbb{1}\otimes V)|\psi\rangle$. Therefore

$$\begin{aligned}\sqrt{q_i}|\phi_i\rangle &= (\mathbb{1}\otimes\langle i|)|\phi\rangle = (\mathbb{1}\otimes\langle i|V)|\psi\rangle \\ &= \sum_j \sqrt{p_j}|\psi_j\rangle\langle i|V|j\rangle = \sum_j V_{i,j}\sqrt{p_j}|\psi_j\rangle,\end{aligned} \tag{4.6}$$

where $V_{i,j} = \langle i|V|j\rangle$. □

4.2 Isometric Extension of Channel

Also a quantum channel admits a purification, called *isometric extension* or *Stinespring dilation* of the channel.

Definition 4.2 (Stinespring dilation)**.** *Let $\Lambda\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ be a quantum channel. A Stinespring isometry V of Λ is an isometry $V \in \mathrm{L}(\mathcal{H}, \mathcal{H}' \otimes \mathcal{H}_R)$ such that*

$$\Lambda[\rho] = \mathrm{tr}_R(V\rho V^\dagger), \tag{4.7}$$

for any density matrix $\rho \in \mathrm{S}(\mathcal{H})$. The isometric channel $\mathcal{E}[\rho] = V\rho V^\dagger$ is called Stinespring dilation of Λ.

In the following, we often use the notation $d = \dim \mathcal{H}$ and $d' = \dim \mathcal{H}'$. By utilizing the Kraus decomposition of a channel, we can employ an orthogonalization procedure akin to the purification of a quantum state to prove the following theorem.

Theorem 4.3 (Stinespring dilation)**.** *Any quantum channel $\Lambda\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ admits an isometric extension with $\dim \mathcal{H}_R \leq dd'$. Moreover, for a channel $\Lambda\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H})$, there exists a pure state $|1\rangle \in \mathcal{H}_R$ and a unitary $U \in \mathrm{L}(\mathcal{H} \otimes \mathcal{H}_R)$ such that*

$$\Lambda[\rho] = \mathrm{tr}_R(U(\rho \otimes |1\rangle\langle 1|)U^\dagger). \tag{4.8}$$

Proof. Let $\Lambda[\rho] = \sum_{i=1}^r K_i \rho K_i^\dagger$ be in Kraus decomposition. We define the operator $V = \sum_{i=1}^r K_i \otimes |i\rangle$ which is element of $\mathrm{L}(\mathcal{H}, \mathcal{H}' \otimes \mathcal{H}_R)$, where the dimension of the space $\mathcal{H}_R$ can be chosen as $\dim \mathcal{H}_R = r = \mathrm{rank}\, J_\Lambda \leq dd'$. Moreover, V is an isometry because

$$V^\dagger V = \sum_{i,j} K_i^\dagger K_j \langle i|j\rangle = \sum_i K_i^\dagger K_i = \mathbb{1}_{\mathcal{H}}. \tag{4.9}$$

Finally, $\mathcal{E}[\rho] = V\rho V^\dagger$ is an isometric extension of Λ since

$$\mathrm{tr}_R(V\rho V^\dagger) = \mathrm{tr}_R(\sum_{i,j} K_i \rho K_j^\dagger \otimes |i\rangle\langle j|) = \sum_i K_i \rho K_i^\dagger = \Lambda[\rho]. \tag{4.10}$$

For the second assertion, we choose the dilation space $\mathcal{H}_R$ of dimension $\dim \mathcal{H}_R = r \leq d^2$. Let $U \in \mathrm{L}(\mathcal{H} \otimes \mathcal{H}_R)$ be a unitary embedding of V into $\mathcal{H} \otimes \mathcal{H}_R$, that is, U is unitary and for the fixed state $|1\rangle \in \mathcal{H}_R$ it satisfies

$$U(|\psi\rangle \otimes |1\rangle) = V|\psi\rangle \tag{4.11}$$

for any $|\psi\rangle \in \mathcal{H}$. Therefore, $V = U(\mathbb{1} \otimes |1\rangle)$, and the Stinespring relation can be written as

$$\Lambda[\rho] = \mathrm{tr}_R(V\rho V^\dagger) = \mathrm{tr}_R(U(\rho \otimes |1\rangle\langle 1|)U^\dagger). \tag{4.12}$$

□

4.3 Naimark Extension of General Quantum Measurement

According to the Stinespring dilation, a quantum channel can be viewed as part of a unitary on a larger system. Similarly, any measurement can be seen as part of a projective measurement, called *Naimark extension*.

Definition 4.3 (Naimark extension)**.** *Let $\boldsymbol{E} = \{E_i\}$ be a POVM on $\mathcal{H}$. A Naimark extension $\boldsymbol{P} = \{P_i\}$ of $\boldsymbol{E}$ is a projective measurement on a Hilbert space $\mathcal{H}'$ of dimension $d' \geq d$, such that*

$$\operatorname{tr}(E_i\rho) = \operatorname{tr}(P_i(\rho \oplus 0)), \tag{4.13}$$

where 0 is the zero matrix of dimension $d' - d$.

The isometric channel $\mathcal{E}[L] = L \oplus 0 \in \mathrm{L}(\mathcal{H}')$ can be understood as an embedding of operators $L \in \mathrm{L}(\mathcal{H})$. It is also possible to use a general isometric channel $\mathcal{E}[L] = TLT^\dagger$ for embedding.

Theorem 4.4 (Naimark extension)**.** *Any n-outcome POVM $\boldsymbol{E}$ on $\mathcal{H}$ admits a Naimark extension $\boldsymbol{P}$ on $\mathcal{H}'$ with $d' = \sum_i \operatorname{rank} E_i$. Moreover, if we choose $\mathcal{H}' = \mathcal{H} \otimes \mathcal{H}_R$ with $\dim \mathcal{H}_R = n$ there exists an orthonormal set $\{|i\rangle \in \mathcal{H}_R\}$ and a unitary $U \in \mathrm{L}(\mathcal{H}')$ such that*

$$\operatorname{tr}(E_i\rho) = \operatorname{tr}(P_i(\rho \otimes |1\rangle\langle 1|)) \quad \textit{with} \tag{4.14}$$

$$P_i = U^\dagger(\mathbb{1} \otimes |i\rangle\langle i|)U. \tag{4.15}$$

Proof. The spectral decomposition of the effects of the POVM $\boldsymbol{E}$,

$$E_k = \sum_l \lambda_{k,l} |e_{k,l}\rangle\langle e_{k,l}|, \tag{4.16}$$

defines a *fine-grained* rank one POVM as

$$\boldsymbol{F} = \{|\psi_i\rangle\langle\psi_i|\}_i, \quad |\psi_i\rangle\langle\psi_i| \coloneqq \lambda_{k,l}|e_{k,l}\rangle\langle e_{k,l}|, \tag{4.17}$$

where $i = i(k,l)$ is a multi-index. The $d' = \sum_i \operatorname{rank} E_i$ vectors $|\psi_i\rangle$ are subnormalized and fulfill $\sum_i |\psi_i\rangle\langle\psi_i| = \sum_k E_k = \mathbb{1}$. Let $\mathcal{H}'$ be a Hilbert space of dimension $d' = \sum_i \operatorname{rank} E_i$ equipped with an orthonormal basis $\{|j\rangle \in \mathcal{H}'\}$. We embed the system space $\mathcal{H}$ into $\mathcal{H}'$ as the subspace spanned by first d basis elements, i.e., $\mathcal{H} \simeq \operatorname{span}\{|j\rangle\}_{j=1}^d$. Define the linear map $\Psi \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ with matrix components such that the vectors $|\psi_i\rangle$ form the matrix rows,

$$\Psi_{i,j} \coloneqq \langle j|\psi_i\rangle, \quad \Psi^\dagger_{i,j} = \langle\psi_j|i\rangle. \tag{4.18}$$

The map Ψ is an isometry, i.e., $\Psi^\dagger\Psi = \mathbb{1}_{\mathcal{H}}$, because

$$[\Psi^\dagger\Psi]_{i,j} = \sum_k \langle\psi_k|i\rangle\langle j|\psi_k\rangle = \sum_k \langle j|\psi_k\rangle\langle\psi_k|i\rangle = \delta_{i,j}. \tag{4.19}$$

The isometry Ψ can be extended to a unitary $\Phi \in \mathrm{L}(\mathcal{H}')$ by completing the set of orthonormal column vectors (spanning $\operatorname{im}\Psi \subseteq \mathcal{H}'$) to an orthonormal basis of $\mathcal{H}'$. In other words, we fill up the columns of the $d' \times d$ matrix Ψ to a unitary $d' \times d'$ matrix $\Phi = (\Psi|*)$. The missing column vectors are obtained from an arbitrary orthonormal basis of $(\operatorname{im}\Psi)^\perp$, or equivalently, from an orthonormal set of $d' - d$ vectors $\{|e_i'\rangle_{i=1}^{d'-d}\}$ satisfying the equation

$$\Psi^\dagger|e_i'\rangle = 0. \tag{4.20}$$

This procedure ensures that Φ has orthonormal rows, which correspond to vectors that orthogonalize the $|\psi_i\rangle$. Define the d' vectors $|\phi_i\rangle$ as the rows of the unitary Φ, that is,

$$\langle j|\phi_i\rangle \coloneqq \Phi_{i,j}. \tag{4.21}$$

These vectors define a Naimark extension $\boldsymbol{P}_F = \{|\phi_i\rangle\langle\phi_i|\}$ of $\boldsymbol{F}$, which is a projective (rank one) measurement satisfying by construction

$$\langle\phi_i|\rho \oplus 0|\phi_i\rangle = \langle\psi_i|\rho|\psi_i\rangle \tag{4.22}$$

for any state $\rho = \sum_{j,k=1}^{d} \rho_{j,k}|j\rangle\langle k| \in \mathrm{S}(\mathcal{H})$, see (4.18) and (4.21). We obtain a Naimark extension of the original POVM $\boldsymbol{E}$ by coarse-graining (relabeling) $\boldsymbol{P}_F$

$$P_k = \sum_l |\phi_{k,l}\rangle\langle\phi_{k,l}|, \tag{4.23}$$

where $k(i), l(i)$ are the original indices from Eq. (4.17). Therefore, $\boldsymbol{P} = \{P_k\}$ is a projective measurement and because of (4.16) and (4.22) a Naimark extension of $\boldsymbol{E}$, i.e., for any state $\rho \in \mathrm{S}(\mathcal{H})$ it holds that

$$\operatorname{tr}(E_i\rho) = \operatorname{tr}(P_i(\rho \oplus 0)). \tag{4.24}$$

We now prove to the second part of the theorem. For practical implementations of the POVM, a tensor product structure is more convenient than a direct sum, as this allows an experimental realization by coupling the system to an ancilla. This ancilla implentation of a POVM can be directly obtained from the previous result by further enlarging the space $\mathcal{H}'$ such that $d' = n \cdot d \geq \sum_i \operatorname{rank} E_i$, where n is the number of outcomes of $\boldsymbol{E}$. Thus, we can impose a product structure $\mathcal{H}' = \mathcal{H}_R \otimes \mathcal{H}$ with $\dim \mathcal{H}_R = n$. As the zero block now has dimension $(n-1)d$, it is possible to write $\rho \oplus 0 = |1\rangle\langle 1| \otimes \rho$, where $|1\rangle$ is the first element of the computational basis

of $\mathcal{H}_R$. Finally, the vectors $|\phi_i\rangle$ from Eq. (4.21) can be embedded in the larger space $\mathcal{H}_R \otimes \mathcal{H}$ as $|\tilde{\phi}_i\rangle := |\phi_i\rangle \oplus 0$ such that we obtain

$$\langle\tilde{\phi}_i|(|1\rangle\langle 1| \otimes \rho)|\tilde{\phi}_i\rangle = \langle\psi_i|\rho|\psi_i\rangle. \tag{4.25}$$

To be more concrete, we now provide an explicit construction of the (basis change) unitary U from the theorem. To match the convention in the literature, we reverse the subsystem order $\mathcal{H}' = \mathcal{H} \otimes \mathcal{H}_R$ such that the ancilla space comes second. Let $\{A_i\}$ be any set of measurement operators for $\boldsymbol{E}$, i.e., $E_i = A_i^\dagger A_i$. We define the operator $V \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ by

$$V = \sum_i A_i \otimes |i\rangle, \tag{4.26}$$

which is an isometry because of the POVM normalization, $V^\dagger V = \sum_i A_i^\dagger A_i = \sum_i E_i = \mathbb{1}_{\mathcal{H}}$. Let $U \in \mathrm{L}(\mathcal{H}')$ be a unitary embedding of V into $\mathcal{H}'$, i.e., U is unitary and for the fixed state $|1\rangle \in \mathcal{H}_R$ it satisfies

$$U(|\psi\rangle \otimes |1\rangle) = V|\psi\rangle \tag{4.27}$$

for any $|\psi\rangle \in \mathcal{H}$. We parameterize the unitary by operators $A_{i,a} \in \mathrm{L}(\mathcal{H})$ as

$$U = \sum_{i,a} A_{i,a} \otimes |i\rangle\langle a|. \tag{4.28}$$

Comparing Eqs. (4.26), (4.27) and (4.28)) implies the consistency condition $A_{i,1} = A_i$. We define the canonical Naimark extension $\boldsymbol{P} = \{P_i\}_{i=1}^n$ of $\boldsymbol{E}$ as

$$P_i = U^\dagger \mathbb{1} \otimes |i\rangle\langle i| U = \sum_{a,b} A_{i,a}^\dagger A_{i,b} \otimes |a\rangle\langle b|, \tag{4.29}$$

which is a (rank-d) projective measurement since $P_i P_j = \delta_{i,j} P_j$. Moreover, every effect of $\boldsymbol{P}$ satisfies

$$\mathrm{tr}(P_i(\rho \otimes |1\rangle\langle 1|)) = \mathrm{tr}(A_{i,1}^\dagger A_{i,1}\rho) = \mathrm{tr}(E_i\rho) \tag{4.30}$$

for any $\rho \in \mathrm{S}(\mathcal{H})$. □

We call $\boldsymbol{P}$ from Eq. (4.13) the *minimal* Naimark extension, and $\boldsymbol{P}$ from Eq. (4.14) the *canonical* Naimark extension of $\boldsymbol{E}$. In the Appendix B we provide the Matlab file `MinNaimark.m` that constructs the minimal Naimark extension of any POVM. Thm. 4.4 can also be interpreted as follows: if the POVM effects are embedded into $\mathrm{H}(\mathcal{H}')$ as $\mathcal{E}[E_i] = E_i \oplus 0$, they can be extended to a projective measurement $\boldsymbol{P}$ on the whole of $\mathcal{H}'$ [BKB18]. In particular, this implies that $\boldsymbol{P}$ and $\mathcal{E}[\boldsymbol{E}]$ have the same expectation values for all embedded states $\mathcal{E}[\rho] = T\rho T^\dagger$, which implies Eq. (4.13):

$$\mathrm{tr}(P_i\mathcal{E}[\rho]) = \mathrm{tr}(\mathcal{E}[E_i]\mathcal{E}[\rho]) = \mathrm{tr}(TE_iT^\dagger T\rho T^\dagger) = \mathrm{tr}(E_i\rho). \tag{4.31}$$

Here, we have used that P_i extends $\mathcal{E}[E_i]$ and that T is an isometry.

CHAPTER 5

Semidefinite Programming

A large number of problems in quantum information theory involve *convex optimization*, where the goal is to minimize a convex function, or maximize a concave function, over a convex set. In particular, the convex sets of quantum states, measurements and channels can be characterized by only linear and semidefinite constraints. If additionally the *objective function*, i.e. the function that is optimized, is linear, the optimization task is called *semidefinite programming*. For semidefinite programs (SDPs) there exists a powerful duality that allows to readily obtain useful bounds on the optimization problem and to make it numerically efficiently solvable. In the following, we describe elements of this theory and discuss selected quantum information tasks involving SDPs that will be used later. This chapter is based on the lecture notes by Watrous [Wat17].

5.1 Primal and Dual Problem

We recall that the space of hermitian operators $\mathrm{H}(\mathcal{H})$ together with the Hilbert-Schmidt scalar product $\langle L, R\rangle = \mathrm{tr}(L^\dagger R)$ defines a real Hilbert space.

Definition 5.1 (SDP)**.** *A semidefinite program is a triple $(A, B, \mathcal{L})$, where $A \in \mathrm{H}(\mathcal{H})$, $B \in \mathrm{H}(\mathcal{H}')$ are hermitian and $\mathcal{L}\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ is a superoperator that preserves hermiticity. The SDP defines the following two optimization problems*

$$\begin{array}{rl} \underline{\text{Primal problem}} & \\ \text{maximize:} & \langle A, X\rangle \\ \text{subject to:} & \mathcal{L}[X] = B \\ & X \in \mathrm{P}(\mathcal{H}) \end{array} \qquad \begin{array}{rl} \underline{\text{Dual problem}} & \\ \text{minimize:} & \langle B, Y\rangle \\ \text{subject to:} & \mathcal{L}^\dagger[Y] \geq A \\ & Y \in \mathrm{H}(\mathcal{H}') \end{array} \tag{5.1}$$

These problems are computational tasks with the aim to maximize $\langle A, X\rangle \in \mathbb{R}$ or minimize $\langle B, Y\rangle \in \mathbb{R}$, subject to the indicated constraints. We call the operators X, Y SDP variables of their respective problem. Moreover, the functions $X \mapsto \langle A, X\rangle$ and $Y \mapsto \langle B, Y\rangle$ are called primal and dual objective function, respectively. From this basic SDP form it is possible to derive seemingly more general problems that include further equality and semidefinite constraints of the SDP variables [Wat17].

An operator $X \in \mathrm{L}(\mathcal{H})$ is called *primal feasible* if it satisfies the primal problem constraints $\{\mathcal{L}[X] = B, X \geq 0\}$. Similarly, an operator $Y \in \mathrm{L}(\mathcal{H}')$ is called *dual feasible* if it satisfies the dual problem constraints $\{\mathcal{L}^\dagger[Y] \geq A, Y^\dagger = Y\}$. The optimal values of the primal and dual problem are denoted by $\alpha, \beta \in \mathbb{R}$, respectively, i.e.,

$$\begin{aligned} \alpha &= \sup\{\langle A, X\rangle : X \text{ is primal feasible}\} \\ \beta &= \inf\{\langle B, Y\rangle : Y \text{ is dual feasible}\}. \end{aligned} \tag{5.2}$$

The following two theorems provide a relation between the primal and dual problems of an SDP.

Theorem 5.1 (Weak Duality)**.** *Let $(A, B, \mathcal{L})$ be an SDP with α, β defined as in Eq. (5.2). It holds that: $\alpha \leq \beta$.*

Proof. In the case that the primal (dual) feasible set ist empty, we set $\alpha = -\infty$ ($\beta = \infty$), and $\alpha \leq \beta$ trivially holds. For any primal feasible operator X and every dual feasible operator Y it holds that

$$\langle A, X\rangle \leq \langle \mathcal{L}^\dagger[Y], X\rangle = \langle Y, \mathcal{L}[X]\rangle = \langle Y, B\rangle = \langle B, Y\rangle. \tag{5.3}$$

Taking the supremum over all primal variables X and the infimum over all dual variables Y yields $\alpha \leq \beta$. □

This theorem implies that any primal feasible operator X yields a lower bound on the optimal dual value β, and any dual feasible operator Y yields an upper bound on the optimal primal value α

$$\langle A, X\rangle \leq \alpha \leq \beta \leq \langle B, Y\rangle. \tag{5.4}$$

An operator $X \in \mathrm{L}(\mathcal{H})$ is called *strictly primal feasible* if it satisfies $\{\mathcal{L}[X] = B, X > 0\}$, where $X > 0$ means that every eigenvalue is positive, $\lambda_i(X) > 0$. Similarly, an operator $Y \in \mathrm{L}(\mathcal{H}')$ is called *strictly dual feasible* if it satisfies $\{\mathcal{L}^\dagger[Y] > A, Y^\dagger = Y\}$.

Theorem 5.2 (Strong Duality)**.** *Let $(A, B, \mathcal{L})$ be an SDP with α, β defined as in Eq. (5.2). It holds that:*

- *$\alpha = \beta$, if the primal feasible set and the strictly dual feasible set are nonempty. Moreover, there exists a primal feasible X such that $\langle A, X\rangle = \alpha$.*
- *$\alpha = \beta$, if the dual feasible set and the strictly primal feasible set are nonempty. Moreover, there exists a dual feasible Y such that $\langle B, Y\rangle = \beta$.*

Strong duality is employed for efficient numerical computation of SDPs, for example, via the open-source MATLAB-based toolbox YALMIP [Löf04] and a suitable solver like SDPT3 [TTT99].

5.2 Optimizing over Measurements

Optimizations of linear functions of POVMs also correspond to an SDP optimization problem. An n-outcome POVM $\boldsymbol{E} = \{E_i\}$ on a d-dimensional Hilbert space $\mathcal{H}$ consists of n positive operators $E_i \geq 0$ that sum to the identity $\sum_i E_i = \mathbb{1}$. An important example of an optimization problem involving POVMs is the *minimum error discrimination* of an ensemble $\{p_i, \rho_i\}$, where the quantum state ρ_i is prepared with probability p_i. The task is to find the optimal measurement $\boldsymbol{E} = \{E_i\}$ such that the probability of obtaining outcome i when ρ_i was prepared is maximized. The figure of merit, the *guessing probability* P_{guess}, is the average probability of successful identification with the optimal POVM. It is given by the solution of the following optimization problem

$$\begin{aligned} P_{\text{guess}} = \quad & \max \sum_i p_i \operatorname{tr}(E_i \rho_i) \\ \text{subject to:} \quad & \sum_i E_i = \mathbb{1}, \\ & E_i \geq 0. \end{aligned} \tag{5.5}$$

We now rewrite this optimization problem to put it into the SDP standard form, Def. 5.1. Let $\mathcal{H}'$ be an n-dimensional Hilbert space with computational basis $\{|i\rangle\}$. Define $\mathcal{L} = \operatorname{tr}_{\mathcal{H}'} \colon \mathcal{H} \otimes \mathcal{H}' \to \mathcal{H}$ to be the partial trace over $\mathcal{H}'$, and define the operators $A \in \mathrm{H}(\mathcal{H} \otimes \mathcal{H}')$ and $B \in \mathrm{H}(\mathcal{H})$ as

$$A = \sum_{i=1}^{n} p_i \rho_i \otimes |i\rangle\langle i| \quad \text{and} \quad B = \mathbb{1}. \tag{5.6}$$

Then, the optimization problem (5.5) can be written in terms of the basic form (5.1) with respect to the SDP $(A, B, \mathcal{L})$ as

$$\begin{array}{lll} & \underline{\text{Primal problem}} & \underline{\text{Dual problem}} \\ P_{\text{guess}} = & \max \langle A, X \rangle & \min \operatorname{tr}(Y) \\ \text{subject to:} & \operatorname{tr}_{\mathcal{H}'}(X) = \mathbb{1} & Y \otimes \mathbb{1} \geq A \\ & X \in \mathrm{P}(\mathcal{H} \otimes \mathcal{H}') & Y \in \mathrm{H}(\mathcal{H}) \end{array} \tag{5.7}$$

Here, we used that the trace over the second subsystem has the adjoint $\operatorname{tr}_B^\dagger(Y) = Y \otimes \mathbb{1}$, which follows from Eq. (2.18). If we make the Ansatz $X = \sum_{i,j} X_{i,j} \otimes |i\rangle\langle j|$, the primal constraints $\operatorname{tr}_{\mathcal{H}'}(X) = \mathbb{1}$ and $X \geq 0$ imply $\sum_i X_{i,i} = \mathbb{1}$ and $X_{i,i} \geq 0$, respectively. Moreover, the scalar product becomes $\langle A, X \rangle = \sum_i p_i \operatorname{tr}(X_{i,i} \rho_i)$. By the identification $E_i = X_{i,i}$, we see that the SDP above (5.7) is equivalent to the optimization (5.5). A useful upper bound to the guessing probability $P_{\text{guess}} \leq \operatorname{tr}(Y)$ is obtained by any dual feasible variable Y, see Eq. (5.4).

5.3 Optimizing over Channels

The optimization of linear functions over the set of channels can be treated with similar methods as before. Let $\mathcal{H}, \mathcal{H}'$ be Hilbert spaces with $d \leq d'$ and let $\Lambda\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ be a channel with Choi matrix $J_\Lambda \in \mathrm{L}(\mathcal{H}' \otimes \mathcal{H})$ given by

$$J_\Lambda = \Lambda \otimes \mathrm{id}[|\Psi\rangle\langle\Psi|] = \frac{1}{d} \sum_{i,j} \Lambda[|i\rangle\langle j|] \otimes |i\rangle\langle j|. \tag{5.8}$$

According to Thm. 3.3, Λ being a channel is equivalent to J_Λ being positive and $\mathrm{tr}_{\mathcal{H}'}(J_\Lambda) = \frac{\mathbb{1}}{d}$. Moreover, because of the one-to-one correspondence of Λ and J_Λ, any real-valued linear function $g(\Lambda) \in \mathbb{R}$ on the set of quantum channels can be expressed by a hermitian operator $G \in \mathrm{H}(\mathcal{H}' \otimes \mathcal{H})$ as

$$g(\Lambda) = \langle G, J_\Lambda \rangle. \tag{5.9}$$

To establish a connection with the SDP standard form (5.1), we define the operators $A = G$, $\mathcal{L} = \mathrm{tr}_{\mathcal{H}'}$ and $B = \frac{\mathbb{1}}{d}$. As a consequence of the Choi theorem 3.3, optimizing a linear function over all channels Λ can be represented by the SDP $(A, B, \mathcal{L})$ whose primal and dual problems are given by

Primal problem		Dual problem	
maximize:	$g(\Lambda) = \langle G, J \rangle$	minimize:	$g(\Lambda) = \frac{1}{d}\,\mathrm{tr}(Y)$
subject to:	$\mathrm{tr}_{\mathcal{H}'}(J) = \frac{\mathbb{1}}{d}$	subject to:	$\mathbb{1} \otimes Y \geq G$
	$J \in \mathrm{P}(\mathcal{H}' \otimes \mathcal{H})$		$Y \in \mathrm{H}(\mathcal{H})$

(5.10)

This SDP has the same form as (5.7), except that $G \in \mathrm{H}(\mathcal{H}' \otimes \mathcal{H})$ is now an arbitrary operator determined by g and not necessarily of block-diagonal form.

5.3.1 Subspace-preserving Channels

In quantum information, a recurring task is the optimization over channels which preserve a number of subspaces, see Ref. [BKB18] for an example. In this section, we provide the necessary background to incorporate such constraints in SDPs.

A superoperator can also be expressed by its coordinate matrix with respect to a fixed basis. This representation has the advantage that the composition of superoperators corresponds to a multiplication of the respective matrices. Let $\mathcal{E}\colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H})$ be a superoperator and let $\mathcal{B} = \{B_\mu\}$ be a Hilbert-Schmidt orthonormal basis of $\mathrm{L}(\mathcal{H})$. The *process matrix* $\hat{\mathcal{E}}$ of $\mathcal{E}$ is defined as the coordinate matrix of $\mathcal{E}$ with respect to $\mathcal{B}$ [Wol12]

$$\hat{\mathcal{E}}_{\mu,\nu} := \langle B_\mu, \mathcal{E}[B_\nu] \rangle = \mathrm{tr}(B_\mu^\dagger \mathcal{E}[B_\nu]). \tag{5.11}$$

By construction, the composition of superoperators $\mathcal{L} = \mathcal{E}_2 \circ \mathcal{E}_1$ corresponds to the matrix multiplication $\hat{\mathcal{L}} = \hat{\mathcal{E}}_2 \hat{\mathcal{E}}_1$. Any CP superoperator is self-adjoint, $\mathcal{E} = \mathcal{E}^\dagger$, if and only if its process matrix is hermitian $\hat{\mathcal{E}} = \hat{\mathcal{E}}^\dagger$ [Wol12]. Given the computational basis $\{|i\rangle\}$ of $\mathcal{H}$, we define the orthonormal *standard basis* of $\mathrm{L}(\mathcal{H})$ as $\mathcal{B} = \{B_\mu = |i\rangle\langle j|\}$, where $\mu = (i, j)$ is a multi-index. This basis permits a direct method to obtain the process matrix by employing the isomorphism (2.20) given by $\mathrm{vec}_{\mathcal{B}}(|i\rangle\langle j|) = |i\rangle \otimes |j\rangle$. When applied to a superoperator $\mathcal{E}[X] = \sum_i L_i X R_i$, this gives the process matrix

$$\hat{\mathcal{E}} = \sum_i L_i \otimes R_i^T . \tag{5.12}$$

In particular, for a completely positive map with Kraus representation $\mathcal{E}[X] = \sum_i K_i X K_i^\dagger$, the process matrix is given by $\hat{\mathcal{E}} = \sum_i K_i \otimes K_i^*$.

Theorem 5.3 (Choi transformation)**.** *Let $\mathcal{E} \colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H})$ be a superoperator with process matrix $\hat{\mathcal{E}}$ with respect to the standard basis of $\mathrm{L}(\mathcal{H})$, and Choi matrix $J_\mathcal{E} \in \mathrm{L}(\mathcal{H} \otimes \mathcal{H})$ (5.8). It holds that $\hat{\mathcal{E}} = d J_\mathcal{E}^R$, where*

$$J_\mathcal{E}^R := \sum_{i,j} (\mathbb{1} \otimes |i\rangle\langle j|) J_\mathcal{E} (|i\rangle\langle j| \otimes \mathbb{1}), \tag{5.13}$$

with $d = \dim \mathcal{H}$. The row-reshuffling operation $L \mapsto L^R$ is called Choi transformation and satisfies $(L^R)^R = L$.

Proof. The row-reshuffling $L \mapsto L^R$ acts on coordinates as $\langle \mu | J_\mathcal{E}^R | \nu \rangle = \langle m, n | J_\mathcal{E}^R | k, l \rangle = \langle m, k | J_\mathcal{E} | n, l \rangle$, where we abbreviate the output and input coordinates as $\mu = (m, n), \nu = (k, l)$, respectively. The definition of the Choi matrix (5.8) yields $d\langle m, k | J_\mathcal{E} | n, l \rangle = \langle m | \mathcal{E}[|k\rangle\langle l|] | n \rangle = \mathrm{tr}(|n\rangle\langle m | \mathcal{E}[|k\rangle\langle l|])$. Putting these together results in:

$$\begin{aligned} d\langle \mu | J_\mathcal{E}^R | \nu \rangle &= \mathrm{tr}(|n\rangle\langle m | \mathcal{E}[|k\rangle\langle l|]) \\ &= \mathrm{tr}(B_\mu^\dagger \mathcal{E}[B_\nu]) = \hat{\mathcal{E}}_{\mu,\nu}. \end{aligned} \tag{5.14}$$

In the last line we used that the standard basis has elements $B_\mu = |i\rangle\langle j|$. □

We now provide an application of Thm. 5.3, that is related to the methods developed in Ref. [BKB18]. Let $S_i \subseteq \mathrm{L}(\mathcal{H})$, $i \in I$ be a sequence of subspaces of the linear operator space, with index set I. We investigate the task of optimizing a linear function $g(\Lambda)$ over channels Λ that are required to preserve the subspaces S_i, i.e., $\Lambda[S_i] \subseteq S_i$ for all $i \in I$. The process matrix allows to readily formulate the subspace-preserving constraint. We define the CPTN superoperator $\mathcal{S}_i[L] := \Pi_i L \Pi_i$, where Π_i denotes the projector onto S_i. A channel Λ preserves the subspace S_i if and only if $\Lambda \circ \mathcal{S}_i = \mathcal{S}_i \circ \Lambda \circ \mathcal{S}_i$, or in terms of the process matrices,

$$\hat{\Lambda}\, \hat{\mathcal{S}}_i = \hat{\mathcal{S}}_i\, \hat{\Lambda}\, \hat{\mathcal{S}}_i. \tag{5.15}$$

Optimizing a linear function over subspace-preserving channels Λ can thus be formulated via the Choi matrix J_Λ and the process matrix $\hat{\Lambda} = dJ_\Lambda^R$ as:

$$\begin{aligned} \text{maximize:} \quad & g(\Lambda) = \langle G, J \rangle \\ \text{subject to:} \quad & J \geq 0, \quad \mathrm{tr}_{\mathcal{H}'}(J) = \tfrac{\mathbb{1}}{d} \\ & J^R \hat{\mathcal{S}}_i = \hat{\mathcal{S}}_i J^R \hat{\mathcal{S}}_i \quad \text{for } i \in I. \end{aligned} \tag{5.16}$$

5.3.2 Quantum Fidelity

We now introduce the *quantum fidelity* as a measure of how close two quantum states are. Given an operator $L \in \mathrm{L}(\mathcal{H}, \mathcal{H}')$ the *trace norm* is defined as

$$||L||_1 = \mathrm{tr}(|L|) = \sum_i s_i(L), \tag{5.17}$$

where $\{s_i(L)\}$ denotes the set of singular values of L (2.25). For positive operators $M, N \in \mathrm{P}(\mathcal{H})$, we define the quantum fidelity as

$$F(M,N) = \left\| \sqrt{M}\sqrt{N} \right\|_1 = \mathrm{tr}\left(\sqrt{M^{1/2} N M^{1/2}}\right). \tag{5.18}$$

Below, we provide a list of some properties of the fidelity. Let $\rho, \sigma \in \mathrm{S}(\mathcal{H})$ be two quantum states and let Λ be a quantum channel. It holds that [NC00]:

- $0 \leq F(\rho,\sigma) \leq 1$ (normalized)
- $F(\rho,\sigma) = F(\sigma,\rho)$ (symmetric)
- $F(\Lambda[\rho], \Lambda[\sigma]) \geq F(\rho,\sigma)$ (monotonic)
- $F(\sum_i p_i \rho_i, \sigma) \geq \sum_i p_i F(\rho_i, \sigma)$ for any probability distribution $\{p_i\}$ and quantum states $\rho_i \in \mathrm{S}(\mathcal{H})$ (concave in both arguments)

These properties qualify the fidelity to be a good measure of "closeness" of two quantum states. If one of its arguments is pure, $\psi = |\psi\rangle\langle\psi|$, the fidelity simplifies to $F(\psi,\rho) = \langle\psi|\rho|\psi\rangle$. Finally, the fidelity can be cast in the form of an SDP [Wat12].

Lemma 5.4 (Fidelity SDP)**.** *The fidelity between two positive operators $M, N \in \mathrm{P}(\mathcal{H})$ is equal to the optimal value of an SDP primal problem given by*

$$\begin{aligned} F(M,N) = \quad & \max \frac{1}{2}(\mathrm{tr}(X) + \mathrm{tr}(X^\dagger)) \\ \text{subject to:} \quad & \begin{pmatrix} M & X \\ X^\dagger & N \end{pmatrix} \geq 0, \\ & X \in \mathrm{L}(\mathcal{H}). \end{aligned} \tag{5.19}$$

CHAPTER 6

Quantum Randomness Generation

The concept of *randomness* has become an integral part of modern science and technologies. The question whether *truly random* events exist in nature is fundamental for science and philosophy. In addition, randomness is nowadays an important resource for numerous applied tasks such as cryptography, algorithms and simulations [AM16].

Until the experimental success of quantum mechanics in the early 20th century, it was believed that nature on the microscopic level is governed by deterministic laws that describe the evolution of any physical system. In a deterministic theory, once the initial conditions of the universe are set, its future can be in principle completely predicted. Consequently, there only exists *pseudorandomness* or *apparent randomness*, where the random behavior of a system emerges because of the incomplete knowledge of its precise microstate [BAK+17].

Probabilistic theories such as quantum mechanics allow for a stronger notion of randomness. There can exist events that *in principle* cannot be predicted with certainty by any knowledge "prior" to the event. We call this notion *true randomness*, *intrinsic randomness* or *private randomness* [Col09]. Here, the word "private" means that degrees of freedom outside the user's safe laboratory, which we collectively call eavesdropper (or Eve), are uncorrelated to the system of interest. True randomness is crucial for any task that requires secrecy, such as cryptography and gambling. Fundamentally, in order to assess how truly random particular data is, one needs to monitor the process of creating the data and its underlying physics.

The probabilistic character of quantum mechanics is evident in the measurement postulate. The measurement of a pure quantum state by a projective measurement (not in the states' eigenbasis) yields outcomes that *even in principle* cannot be perfectly predicted by any observer. In current quantum technologies, this feature is exploited to generate truly random numbers (see, e.g., www.idquantique.com). However, in any realistic setting true randomness is mixed with apparent randomness due to noise or a mismatch between theoretical description and actual implementation. The challenging task in the field of *quantum randomness generation* is to quantify the amount of true randomness produced in a quantum protocol, while keeping the assumptions experimentally viable.

6.1 Randomness Expansion

In this thesis, we focus on one of the two important kinds of quantum randomness protocols, namely on *randomness expansion* [Col09, CK11]. Here, the aim is to start with a perfectly private random string and generate a longer one, in a way that guarantees that the longer string is also kept private from the eavesdropper during the execution of the protocol. A more precise definition will be given at the end of this section, when we will have established the necessary concepts. In subsequent sections, we decribe how randomness expansion can be performed employing quantum mechanics. The other important type of protocol is called *randomness amplification* or *randomness extraction* from weak sources. Here, the user has only imperfect randomness at his disposal and aims at distilling fully random bits from it [GMDLT$^+$13, KAF17]. This task is similar to privacy amplification in quantum cryptography [Ren08, SBPC$^+$09]. However, the latter is usually performed using *seeded* extractors, which require a small amount of perfect randomness from the start, see Sec. 6.1.2.

Data obtained from unpredictable events is not useful for a subsequent task, if it is immediately broadcasted to the eavesdropper. In order for randomness expansion to be useful before employing, for example, a cryptographical protocol, assumptions about the privacy of the laboratory and the devices in it are needed. Therefore, we set the following assumptions valid for the rest of the discussion.

Randomness Expansion Assumptions:

1. The randomness expansion protocol takes place in a laboratory that during the execution of the protocol is shielded from any information transfer to the outside.

2. The user possesses secure classical information processing devices in the laboratory, that allow for the processing of classical data without leakage to the eavesdropper.

3. The devices and their surroundings function according to the laws of quantum mechanics.

These assumptions allow the user to reuse randomness that was utilized for the classical information processing in the laboratory. However, one needs to ensure that the generated data is uncorrelated to the randomness that is initially held. Quantum key distribution (QKD) [SBPC$^+$09] describes the task where two or more parties establish correlated random data. Compared to QKD, in randomness generation no correlations with a remote party are needed, and thus, no classical information is leaked to the eavesdropper (for error correction) until the data is utilized in a task.

Further assumptions are often made depending on the concrete protocol at hand. For example, so-called device-independent protocols [Col09, PAM+10, LZL+18] require a stronger version of the first assumption, namely that the laboratory contains sub-laboratories that can be shielded from each other. This is necessary to ensure causal separation of the measurement devices.

6.1.1 True Randomness

A formal and quantitative definition of true randomness can be provided via the notion of spacetime quantum states [FRT13]. These are states with an associated four-vector that describes the physical location of the state in relativistic spacetime. We interpret the spacetime coordinate of ρ as the event where the process generating ρ is started. Moreover, we describe side information, i.e., any additional system correlated to ρ, by spacetime states. In this case, the four-vector indicates when and where this information is accessible. By means of Eq. (3.11) we directly obtain a notion of spacetime random variables.

Definition 6.1 (True randomness)**.** *A random variable X with alphabet $\mathcal{X}$ is called ε-random if for any system E, the CQ-state ρ_{XE} is ε-close to a state that is uniform and uncorrelated to any space time state ρ_E not in the future light cone of ρ_X:*

$$\frac{1}{2}\left\|\rho_{XE} - \frac{\mathbb{1}}{|\mathcal{X}|} \otimes \rho_E\right\|_1 \leq \varepsilon. \tag{6.1}$$

Here, $||L||_1 = \mathrm{tr}(|L|)$ denotes the trace norm of L. We call X fully random if ε is not larger than a predefined small treshold value, $\varepsilon \leq \bar{\varepsilon} \ll 1$.

The definition above captures the idea that a variable is truly random if it is uncorrelated to any information that does not lie in the causal future of it. Certainly, particular systems in the causal future of ρ are highly correlated with it. This is why the safe-laboratory assumption is crucial: it prevents Eve from learning the value of X by just broadcasting it after its generation. Her power is (necessarily) restricted to establish correlations with systems in the "past" of the process that generates ρ. In the definition above, the (normalized) trace distance $D(\rho,\sigma) = \frac{1}{2}||\rho - \sigma||_1$ is chosen as distance measure as it has the operational interpretation as *distinguishing advantage*. If two equiprobable quantum states are ε-close to each other in trace distance, the success probability of distinguishing them by a measurement is at most $\frac{1}{2}(1+\varepsilon)$ [NC00]. Thus, one can consider the two scenarios described by them as identical except with probability ε. Consequently, a fully random variable X can be considered completely unpredictable, except for a small failure probability $\bar{\varepsilon}$. This property of the trace distance is at the root of the universally *composable* security framework in quantum cryptography [RK05], which ensures that a cryptographic protocol is secure in any arbitrary context. For example, a bit of X remains secret even if some other part of X is given to the adversary.

6.1.2 Quantum Entropies and Randomness Extraction

The raw output of any realistic, physical random number generator is almost certainly not fully random. However, perfect randomness can be distilled from the output via post-processing called *randomness extraction* or *privacy amplification*. A randomness extractor takes an initial string X, about which a potential adversary has partial knowledge E, and compresses it to a shorter string X', which is fully random. The compression rate is determined by the *min-entropy* [Ren08], which we describe below.

Let A, B be two quantum systems and ρ_{AB} a joint quantum state. The *min-entropy* of ρ_{AB} given the side information $\sigma_B \in \mathrm{S}(\mathcal{H}_B)$ is defined as

$$H_{\min}(A|\sigma_B)_\rho = \sup\{\lambda \in \mathbb{R} : \rho_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B\}. \tag{6.2}$$

There exists a feasible λ only if $\operatorname{supp} \sigma_B \supseteq \operatorname{supp} \rho_B$ [Tom12]. The min-entropy of A given B on the state ρ_{AB} is defined via the *optimal* side information

$$H_{\min}(A|B)_\rho \coloneqq \max_{\sigma_B \in \mathrm{S}(\mathcal{H}_B)} H_{\min}(A|\sigma_B)_\rho. \tag{6.3}$$

If the first system is classical, $A = X$, the state ρ_{XB} is a CQ-state (3.12). In this case, the min-entropy can be related to the maximal probability of guessing the random variable X given quantum side information B [KRS09]

$$H_{\min}(X|B) = -\log P_{\text{guess}}(X|B), \tag{6.4}$$

with the guessing probability from Eq. (5.5). This relation provides an operational meaning to the min-entropy. Similar to the guessing probability, the general min-entropy can be evaluated by an SDP (5.7), making it accessible for efficient numerical computation [Tom12].

The quantum min-entropy obeys a duality relation with the quantum *max-entropy*, which can be used to define the max-entropy as follows [KRS09]. Let ρ_{AB} be a quantum state with purification $|\psi\rangle_{ABC}$. We define the max-entropy of A given B on the state ρ_{AB} as

$$H_{\max}(A|B) \coloneqq -H_{\min}(A|C). \tag{6.5}$$

Another important quantity is the *von Neumann entropy* of a state ρ, which is defined as

$$S(\rho) \coloneqq -\operatorname{tr}(\rho \log \rho). \tag{6.6}$$

The *conditional* von Neumann entropy of A given B on the state ρ_{AB} is defined as

$$S(A|B)_\rho \coloneqq S(\rho_{AB}) - S(\rho_B). \tag{6.7}$$

As the labels suggest, for any state ρ_{AB} it holds that

$$H_{\min}(A|B) \leq S(A|B) \leq H_{\max}(A|B). \tag{6.8}$$

Some bounds in information theory can be made (almost) tight by employing a *smoothed* version of the entropies [Ren08, TCR09]. Given two positive operators $\rho, \hat{\rho}$, the *purified distance* is defined as $P(\rho, \hat{\rho}) := \sqrt{1 - F^2(\rho, \hat{\rho})}$ with the quantum fidelity $F(\rho, \hat{\rho})$ from (5.18). The purified distance is a metric on the space of subnormalized quantum states [TCR10]. For any $\varepsilon > 0$, the ε-ball around a state $\rho \in \mathrm{S}(\mathcal{H})$ is given by

$$\mathcal{B}_\varepsilon(\rho) := \{\hat{\rho} \in \mathrm{P}(\mathcal{H}) : P(\rho, \hat{\rho}) \leq \varepsilon, \mathrm{tr}(\hat{\rho}) \leq 1\}. \tag{6.9}$$

With that, the smooth conditional min-entropy of A given B on the state $\rho_{AB} \in \mathrm{S}(\mathcal{H}_{AB})$ is defined as

$$H^\varepsilon_{\min}(A|B)_\rho := \max_{\hat{\rho} \in \mathcal{B}_\varepsilon(\rho)} H_{\min}(A|B)_{\hat{\rho}}. \tag{6.10}$$

The smooth min-entropy plays an important role in quantifying the extractable randomness in data. We now describe the important case of randomness extraction via *two-universal hashing*, where the hash (extraction) function is chosen from the following class. A set of functions $\mathcal{F}$ from $\mathcal{X}$ to $\mathcal{X}'$ with $|\mathcal{X}'| = 2^l$ is called *two-universal* if: for any $f \in \mathcal{F}$ chosen uniformly at random and for any distinct instances $x_1 \neq x_2 \in \mathcal{X}$, it holds that

$$\Pr(f(x_1) = f(x_2)) \leq \frac{1}{2^l}. \tag{6.11}$$

In other words, the probability that the hash function maps x_1, x_2 to the same value of $\mathcal{X}'$ is bounded from above. It has been shown that a two-universal set $\mathcal{F}$ can be chosen with size $|\mathcal{F}| = |\mathcal{X}|$ [CK11]. In practice, the hash function $f \in \mathcal{F}$ is drawn by making use of a small fully random seed, which ensures that the eavesdropper (and the quantum devices) do not know f in advance. If the user has only partial randomness at his disposal, security is not guaranteed. Therefore, two-universal hashing as formulated in the following Lemma belongs to the class of *seeded* extractors [Ren08].

Lemma 6.1 (Leftover hashing)**.** *Let ρ_{XE} be a CQ-state and let $\mathcal{F}$ be a two-universal family of hash functions from $\mathcal{X}$ to $\mathcal{X}'$ with $|\mathcal{X}'| = 2^l$. If we denote the quantum registers of $\mathcal{X}'$ and $\mathcal{F}$ as X' and F, respectively, it holds that*

$$\frac{1}{2}\left\|\rho_{X'EF} - \frac{\mathbb{1}}{2^l} \otimes \rho_{EF}\right\|_1 \leq \varepsilon + \frac{1}{2} 2^{-\frac{1}{2}(H^\varepsilon_{\min}(X|E) - l)} =: \varepsilon + \varepsilon_h,$$

where $\rho_{X'EF}$ is the average joint state after randomly applying the hash function,

$$\rho_{X'EF} = \sum_{f \in \mathcal{F}} \frac{1}{|\mathcal{F}|} \rho_{f(X)E} \otimes |f\rangle\langle f|.$$

Note that the inclusion of the register F in the state ensures that $X' = f(X)$ is uniform from Eve's point of view even if she learns the function f. Lemma 6.1 states that for a fixed length l of the output string, ε_h decays exponentially in $H_{\min}^{\varepsilon}(X|E)$ and thus the randomness quality increases. Moreover, for the choice $l = H_{\min}^{\varepsilon}(X|E) - t$ with $t \geq 0$ such that $\delta := \varepsilon + \frac{1}{2}2^{-t/2} \leq \bar{\varepsilon}$, the output $X' = f(X)$ of the hash function is fully random, i.e., uniform and independent of E except with probability $\bar{\varepsilon} \ll 1$. Thus, for large $|\mathcal{X}|$, the min-entropy $H_{\min}^{\varepsilon}(X|E)$ is roughly equal to the number of fully random bits that can be extracted from X. With that, we are ready to give a more precise definition of a randomness expansion protocol [BKB17].

Quantum Randomness Expansion: a quantum randomness expansion scheme is any protocol satisfying at least the assumptions 6.1, and consists of the following steps. An honest user possesses a fully random initial bit string $\boldsymbol{A}$. The user supplies a certain number of bits from $\boldsymbol{A}$ roundwise to quantum devices that provide the bit string $\boldsymbol{X}$ as joint output. The remaining bits of $\boldsymbol{A}$ are employed for two-universal hashing of $\boldsymbol{X}$ to obtain a compressed string $\boldsymbol{X}'$ which is fully random, conditioned on $\boldsymbol{A}$ as well as on any side information E previously stored in the devices. The protocol outputs the fully random concatenated string $(\boldsymbol{A}, \boldsymbol{X}')$.

We can interpret the additional randomness $\boldsymbol{X}'$ as being generated by the intrinsic unpredictability of quantum mechanics. Hence, we use the term *randomness generation* synonymously with randomness expansion.

6.2 Accumulated Entropy

As we described in the previous section, the main step in a randomness generation protocol is to establish a nontrivial lower bound on the conditional min-entropy $H_{\min}(\boldsymbol{X}|\boldsymbol{C}E)$. Here, $\boldsymbol{X}$ denotes the raw output of the quantum devices, $\boldsymbol{C}$ denotes any classical data except $\boldsymbol{X}$ that is used or generated in the protocol, and E denotes the eavesdropper's degrees of freedom. Since randomness generation protocols consist of a large number of identical rounds, the usual strategy to bound $H_{\min}(\boldsymbol{X}|\boldsymbol{C}E)$ is divided into two parts:

i) The min-entropy of all rounds $H_{\min}(\boldsymbol{X}|\boldsymbol{C}E)$ is related to a suitable single-round entropy, by making use of assumptions about the eavesdropper's power and the physical setup.

ii) The single-round conditional entropy is bounded by employing assumptions about the physical setup.

In this section we discuss step i), while step ii) will be described in the next section. One assumption commonly used to simplify task i) is that in an n-round protocol, the bits of $\boldsymbol{X} \equiv X^n = (X_1, \ldots, X_n)$ are created independently from each other in the same way. That is, the adversary employs an *independent and identically distributed* (IID) attack: in every round of the protocol the quantum devices make the same measurement on the same quantum state. Consequently, both the shared state between the user and Eve at the beginning of the protocol and the measurements have tensor product form [AFRV16]. This implies that the joint quantum state ρ_{XE}^n after n rounds is the n-fold tensor product of a single round state

$$\rho_{XE}^n = \rho_{XE}^{\otimes n}. \tag{6.12}$$

We call a state of the form (6.12) an IID state. In this case, there are simple means to relate the total entropy of X^n to single-round entropies depending on X_i. The easiest variant of such an argument leads to the following bound for any $\varepsilon \geq 0$

$$H_{\min}^{\varepsilon}(X^n|E^n)_{\rho^{\otimes n}} \geq H_{\min}(X^n|E^n)_{\rho^{\otimes n}} = nH_{\min}(X|E)_{\rho}. \tag{6.13}$$

The inequality holds because $H_{\min}(X|E) = H_{\min}^{\varepsilon=0}(X|E)$. The equality follows from the additivity of the min-entropy [Ren08]. However, the bound (6.13) is usually too pessimistic. If we accept a small failure probability, a tigher bound for IID states (6.12) can be derived based on smooth entropies. The improvement is provided by the *quantum asymptotic equipartition property* (AEP) [TCR09].

In classical information theory the AEP is a central result because it allows to characterize the *typical* behaviour of IID random variables in terms of the *Shannon entropy*. The Shannon entropy of a random variable $X = \{p_x, x\}$ is given by

$$H(X) = -\sum_{x \in \mathcal{X}} p_x \log p_x. \tag{6.14}$$

The classical AEP states that, for large enough n, the outcome of a random experiment given by an IID sequence of random variables $X^n = (X_1, \ldots, X_n) \in \mathcal{X}^{\times n}$, where X_i is distributed according to $\{p_x\}$, will almost certainly be in a set of approximately $2^{nH(X)}$ typical events that each occur with a probability close to $2^{-nH(X)}$. This result can be derived from the law of large numbers. As a consequence, e.g., for source compression only $2^{nH(X)}$ bits are needed to store the whole sequence X^n if we accept a small failure probability for non-typical events. The quantum generalization of $H(X)$ is the von Neumann entropy $S(\rho)$ (6.6), which plays a similar role as described by the quantum AEP [AF18].

Theorem 6.2 (Quantum AEP)**.** *Let $\rho_{AE} \in \mathrm{S}(\mathcal{H}_{AE})$ and $\varepsilon > 0$. For the IID state $\rho_{AE}^{\otimes n}$ with large enough $n \in \mathbb{N}$, it holds that*

$$H_{\min}^{\varepsilon}(A^n|E^n)_{\rho^{\otimes n}} \geq nS(A|E)_{\rho} - \sqrt{n}\delta(\varepsilon, \nu), \tag{6.15}$$

where the second term is given by

$$\delta(\varepsilon,\nu) = 4\log\nu\sqrt{\log(2/\varepsilon^2)}, \quad \textit{with} \quad \nu = 2\sqrt{2^{H_{\max}(A|E)}} + 1. \tag{6.16}$$

Note that δ is independent of n and thus the term $\sqrt{n}\delta$ can be neglected in the large n limit. Moreover, the AEP bound is independent of $\dim \mathcal{H}_E$, which is important for randomness generation as the dimension of the adversary's quantum system cannot be bounded. The quantum AEP establishes the von Neumann entropy as the relevant quantity for problems involving IID states and usually leads to significantly better bounds than (6.13). On the other hand, in partially-characterized setups, the single-round von Neumann entropy is usually harder to bound compared to the single-round min-entropy. This is because the former is non-linear, while the latter can be derived from the linear guessing probability (6.4).

In the following, we focus on the IID asymptotic case, that is, we assume that Eve performs an IID strategy and consider the limit of an infinite number of rounds $n \to \infty$. This relevant idealization is often employed in the literature because it simplifies the analysis, as finite-statistics effects do not need to be taken into account. In this case, the quantum AEP can be formulated as follows [Ren08]. For an an IID state $\rho_{AE}^{\otimes n}$ with $n \in \mathbb{N}$ it holds that

$$\begin{aligned} \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{\min}^{\varepsilon}(A^n|E^n)_{\rho^{\otimes n}} &= S(A|E)_\rho \quad \text{and} \\ \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{\max}^{\varepsilon}(A^n|E^n)_{\rho^{\otimes n}} &= S(A|E)_\rho. \end{aligned} \tag{6.17}$$

Moreover, when relaxing the IID assumption, the single-round von Neumann entropy can still be related to the min-entropy of all rounds via: i) the *quantum de Finetti theorem* [CFS02, Ren08] ii) the *entropy accumulation theorem* [AFDF$^+$18]. These results essentially imply that in the asymptotic case an IID strategy is optimal for the adversary.

6.3 Quantum Random Number Generators

Quantum random number generators (QRNGs) exploit the intrinsic probabilistic nature of quantum mechnics to generate truly random numbers. A QRNG is a device where a quantum state ρ is measured by a POVM $\boldsymbol{F} = \{F_x\}$. The *raw randomness* is the random variable X of the measurement results, where the outcome $X = x$ occurs with probability

$$p_x = \mathrm{tr}(F_x\rho). \tag{6.18}$$

Quantum mechanics predicts that if we measure a pure quantum state by a projective measurement not in the state's eigenbasis, the outcomes of X cannot be fully

predicted, i.e., X contains true randomness. However, any realistic QRNG contains some amount of noise due to couplings with the environment, i.e., ρ is not pure and $\boldsymbol{F}$ is not projective. As a consequence, Eve can gain additional information about X. The security analysis of a QRNG bounds the maximal amount of information that Eve obtains about X given some assumptions about the devices. As described by Eq. (6.15), this amounts to establishing a lower bound on the single-round entropy $S(X|E)_\rho$ (6.7). Thus, we define the (IID asymptotic) randomness generation rate as

$$R_{X|E} = S(X|E)_\rho, \tag{6.19}$$

where X is the outcome variable of the POVM $\boldsymbol{F}$ (6.18). If Eve only possesses side information about the measured state and not the POVM, we say that the noise in the measurement is trusted (see later). In this case, the randomness generation rate is given by a quantity called *relative entropy of POVM-based coherence* [BKB19]. That is, $R_{X|E} = C_{\text{rel}}(\rho, \boldsymbol{F})$, where

$$C_{\text{rel}}(\rho, \boldsymbol{F}) = H(X) + \sum_x p_x(\rho) S(\rho_x) - S(\rho), \tag{6.20}$$

with $p_x(\rho) = \text{tr}(F_x \rho)$, $\rho_x = A_x \rho A_x^\dagger / p_x$ and $A_x = \sqrt{F_x}$. Here, $S(\rho)$ denotes the von Neumann entropy (6.6) and $H(X)$ denotes the Shannon entropy (6.14). In Fig. 6.1 below we visualize this type of QRNG.

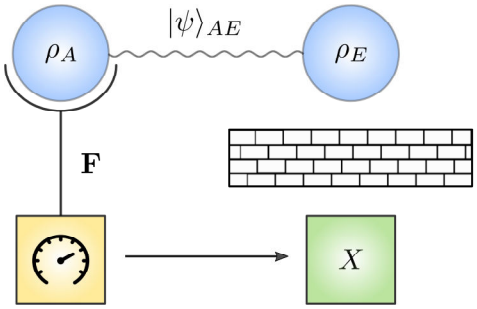

Figure 6.1: A QRNG where the noise in the measurement is trusted. Eve has maximal side information about the measured state ρ_A, that is, she holds the system E of a purification $|\psi\rangle_{AE}$. If ρ_A is measured by a POVM $\boldsymbol{F}$, the measurement outcomes $X = x$ contain private randomness with respect to Eve. The IID asymptotic randomness generation rate is given by $R_{X|E} = C_{\text{rel}}(\rho_A, \boldsymbol{F})$, with the relative entropy of POVM-based coherence defined in Eq. (6.20).

The amount of certifiable randomness depends on the level of characterization of the devices and on the assumption on the adversary's power [LBS14]. The following list contains assumptions that can be used to classify most existing randomness generation protocols.

Characterization of state/measurement: The state (measurement) of the QRNG can be either fully characterized or uncharacterized. There also exist works where partial characterizations are employed, e.g., the Hilbert space dimension is upper bounded, or states (measurements) are restricted to a particular subset.

Trusted/Untrusted noise: We call any noise present in a characterized state (measurement) *untrusted*, if Eve holds a quantum system correlated with it, e.g., a purifying system. We call noise *trusted* if Eve does not have accesss to correlated degrees of freedom. In the latter case, the user may need to utilize initial randomness to ensure that the noise is trusted.

Classical/Quantum adversary: The adversary is called *classical* if Eve must measure her side information before the classical postprocessing (e.g., randomness extraction) of the protocol. The adversary is called *quantum* if Eve holds quantum side information. This enables her to store the information in a quantum memory and delay her measurement until any later time convenient for her, e.g., when the randomness is used for a subsequent protocol. She can then perform the best measurement determined by her knowledge, which in general is a joint measurement on all of Eve's quantum side information.

To provide an example, we describe the assumptions made in *standard* quantum key distribution [SBPC$^+$09]. In this case, one assumes characterized and trusted measurement devices and an uncharacterized shared state. Moreover, an IID attack of a classical adversary is called an *individual attack*, while an IID attack of a quantum adversary is called a *collective attack*.

With the classification above, we can discuss the most common theoretical schemes for QRNGs, which are shown in Table 6.1. The levels of characterization are ordered from strongest to weakest assumption.

	State	Measurement
Device-dependent	$\checkmark_u$	$\checkmark_t$
Source-device-independent	$\times$	$\checkmark_t$
Measurement-device-independent	$\checkmark_t$	$\times$
Semi-device-independent	$\times^*$	$\times^*$
Device-independent	$\times$	$\times$

Table 6.1: Frameworks for quantum randomness generation with different levels of characterization of state and measurement (see the main text for details). The symbol $\checkmark_t$ means characterized and with trusted noise, $\checkmark_u$ means characterized and with untrusted noise, $\times$ means uncharacterized, while $\times^*$ means uncharacterized except an upper bound on the Hilbert space dimension.

Device-dependent schemes explicitly model the devices used in the QRNG [AAM+15, BAK+17]. Typical off-shelf and practical devices belong to this class. These QRNGs usually apply statistical tests on the output bits to ensure unpredictability. In *source-device-independent* (SDI) schemes one assumes a trusted measurement device and a completely untrusted source of quantum states [CZYM16, MVV17, AMVV18]. Here, usually entropic uncertainty relations between quantum observables are used to obtain some bound on the conditional min-entropy.

Following the observation that detectors are particularly susceptible to side-channel attacks, the *measurement-device-independent* (MDI) level of characterization has been proven to be very successful in practical QKD [LCQ12, TYC+14]. MDI QRNGs consist of a characterized state source and a completely uncharacterized measurement device [CZM15, NGZ+16, BKB17]. We describe and analyze this scheme in the subsequent section.

Moreover, there exist various further schemes with an intermediate level of characterization, where different types of certifying *quantumness* are used to quantify generated randomness. This includes QRNGs based on quantum steering [PCSA15, GMG+18], quantum contextuality [UZZ+13] or the maximum overlap of emitted states [BME+16]. In particular, *semi-device-independent* schemes [LYW+11, LBL+15] assume uncharacterized devices with an upper bound on their Hilbert space dimension.

Finally, *device-independent* (DI) schemes promise the highest level of security by viewing all QRNG devices as black boxes with a classical interface [Col09, AFDF+18, LZL+18]. Randomness is certified via the violation of a Bell-type inequality, which requires a loophole-free Bell test setup. While loophole-free Bell violations have been reported, the complexity of these setups makes DI QRNGs rather impractical [BKG+18].

6.4 Measurement-device-independent Randomness Generation

In this section, we describe measurement-device-independent (MDI) randomness generation, which is a family of QRNGs with an intermediate level of characterization, see Table 6.1. The content of this section is a summary of the results in my publication Ref. [BKB17]. The original publication and my precise contribution to this work can be found in the Appendix A.1.

6.4.1 Summary of Results

The role of general measurements for quantum randomness generation was studied in Ref. [BKB17]. We investigated a general MDI QRNG setup, consisting of two

devices: any well-characterized state source and a completely uncharacterized detector. The setup is shown in Fig. 6.2. In every round, the characterized state source upon receiving the input a emits the quantum state $\rho(a)$ from a fixed set $\{\rho(a)\}$. The uncharacterized detector announces an outcome x whenever a state was sent. We denote by $P_{\text{obs}}(x,a)$ the probability that the pair (x,a) occurs, which is estimated after a large number of rounds. The knowledge of $\{\rho(a), P_{\text{obs}}(x,a)\}$ can be used to bound the amount of side information that Eve may have about the detector outcomes.

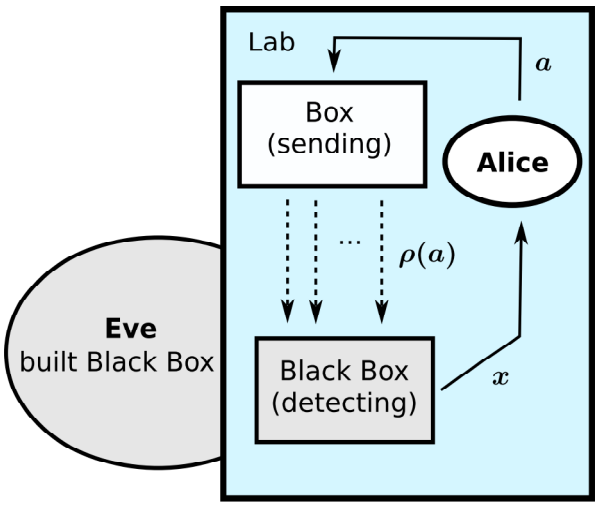

Figure 6.2: The measurement-device-independent setup for randomness generation. The trusted source sends for the input $a \in \{1,\ldots,n_s\}$ a known state $\rho(a)$ to an untrusted measurement device, which outputs x with $x \in \{1,\ldots,n_o\}$. The outcome randomness $\mathcal{R}_X$ is characterized by the observed probability distribution $P_{\text{obs}}(x,a)$, i.e. the probability that the pair (x,a) occurs. This figure is taken from my publication [BKB17].

We formulated a randomness expansion protocol, describing how the inital random string A is employed together with the quantum states and measurement device to obtain the raw randomness [BKB17]. The latter is described by the single-round random variable X with outcomes x. Under the randomness expansion assumptions from Sec. 6.1 and for the IID asymptotic case, we performed a detailed analysis of the eavesdropper's degrees of freedom in any MDI QRNG setup. This is used to characterize the generation rate $\mathcal{R}_X$ of fresh random bits. Here, $\mathcal{R}_X = H_{\min}(X|AE)$ is the single-round min-entropy, characterizing the unpredictability of measurement outcomes with respect to the utilized randomness A and Eve E. It holds that $H_{\min}(X|AE) = -\log P_{\text{guess}}(X|AE)$, see Eq. (6.4). Moreover, the single-round entropy $H_{\min}(X|AE)$ is connected to the min-entropy of all rounds by virtue of Eq. (6.13).

The following main result is proven in [BKB17]. The guessing probability

$P_{\text{guess}}(X|AE)$ in any MDI QRNG setup is characterized by the following SDP:

$$\begin{aligned} P_{\text{guess}}(X|AE) \leq & \max_{\{M_{x,e|a}\}} \sum_{x,a} p_a \operatorname{tr}(M_{x,x|a}\rho(a)) \\ \text{s.t.} \quad & M_{x,e|a} \geq 0, \quad \sum_{x,e} M_{x,e|a} = \mathbb{1} \quad \forall a, \\ & P_{\text{obs}}(x,a) = \sum_{e} p_a \operatorname{tr}(M_{x,e|a}\rho(a)) \\ & + \text{ Further linear constraints.} \end{aligned} \tag{6.21}$$

Here, $p_a = \sum_x P_{\text{obs}}(x,a)$ is the probability that $\rho(a)$ was sent. The second line means that the optimization variable $\{M_{x,e|a}\}$ is a POVM with outcomes (x,e) for each a. The third line ensures that the adversary's operations actually give rise to the observed measurement statistics P_{obs}. The omitted constraints can be interpreted as nonsignalling conditions between the detector and Eve's site E, and between the systems A and E, respectively.

In Ref. [BKB17], the general characterization (6.21) was then used to study various specific MDI QRNGs defined by $\{\rho(a), P_{\text{obs}}(x,a)\}$. In particular, the findings include setups that yield the maximally achievable randomness generation rate of $\mathcal{R}_X = 2\log d$ bits per round, where $d = \dim \mathcal{H}$ is the dimension of the Hilbert space. Hence, for fixed d, (extremal) POVMs can yield up to twice the randomness generation rate compared to projective measurements, see Fig. 6.3. This demonstrates the advantage of general quantum measurements over projective measurements in quantum random number generation. Moreover, Fig. 6.3 shows that the usage of additional linearly independent states $\rho(a)$ yields an improvement of the randomness generation rate for noisy detectors (quality $\eta < 1$). The string of raw randomness $\boldsymbol{X}$ encompasses the outcomes of X after all rounds of the protocol. The user can employ two-universal hashing (Lemma 6.1) to transform $\boldsymbol{X}$ to a string $\boldsymbol{X}'$ that is fully random, see Def. 6.1.

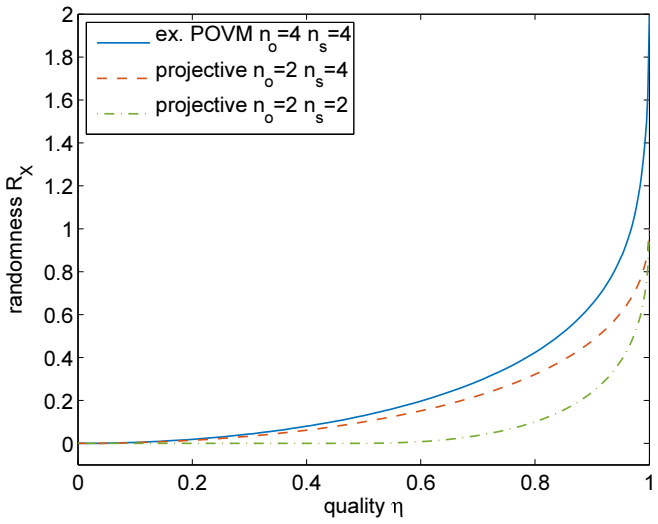

Figure 6.3: The randomness rate versus the detector quality for an optimal qubit setup (see Ref. [BKB17] for details). Here, η is a quality parameter that is inversely proportional to the amount of white noise in the measurement statistics. The solid (dashed) line depicts an extremal POVM with $n_o = 4$ ($n_o = 2$) outcomes for an informationally complete set of $n_s = 4$ states. The dash-dotted line corresponds to the case of two non-orthogonal sent states and two outcomes. This figure is taken from my publication [BKB17].

CHAPTER 7

Resource Theory of Quantum Coherence

Quantum information theory can be understood as a theory of interconversion of different resources. In particular, it describes how quantum properties (resources) enable superior performance in certain information tasks compared to classical physics. *Quantum resource theories* (QRTs) offer a versatile, application-independent, methodological framework for the quantitative analysis of different quantum phenomena.

The main insight of resource theories is that under given constraints, particular operations become very costly compared to others. Such constraints are present in most physical setups and stem from either practical, experimental limitations or the laws of physics. Consequently, only a subset of operations can be (easily) realized, which are called *free operations*. Properties of quantum states that cannot be created by free operations are considered a valuable resource. States without resource content are called *free states* and can often be prepared by free operations from any state. Conversely, quantum states carrying resource can be employed to (partially) circumvent the restrictions on the free operations, i.e., to realize general operations. Building solely on free states and operations, it is possible to develop a rigorous, quantitative QRT framework. This provides insights into the different means of quantifying a resource, the optimal distillation and dilution of the resource and the rate of interconversion of resource states under the given constraints.

The first resource theory was formulated to provide a quantitative theory of entanglement [HHH$^+$03, HHHH09]. In recent years, the QRT framework has been applied to other quantum information concepts such as coherence [BCP14, WY16] and purity [HHO03]. QRTs also play a role in broader research areas, including asymmetry [GS08] and thermodynamics [BHO$^+$13]. In the latter case, the resource-theoretic viewpoint has been proven especially useful, as it avoids problematic and ambiguous quantum generalizations of classical concepts such as heat and entropy as its starting point [KJJ$^+$18].

7.1 General Structure of Resource Theories

In the present time, there exists an increasing number of results on general quantum resource theories, see [BG15, CFS16, LHL17, CG19] for an overview. In this section, we discuss basic definitions and consistency properties of general QRTs. Further topics such as resource quantification and manipulation will be treated later in the resource theory of coherence.

A resource theory is based on two main concepts, free channels and free states. In this thesis, we only consider operations (channels) with the same input and output space $\mathrm{L}(\mathcal{H})$ which suffice for the resource theory of coherence. In the following, we usually suppress the dependence of all quantities on the underlying Hilbert space $\mathcal{H}$.

Definition 7.1 (Resource-free operations)**.** *A subset $\mathcal{O}$ of the set of all channels from $\mathrm{L}(\mathcal{H})$ to itself is called a set of free operations if:*

1. *for any Hilbert space $\mathcal{H}$, $\mathcal{O}$ contains the identity map* id
2. *for free operations $\Lambda, \Lambda' \in \mathcal{O}$ the composition $\Lambda \circ \Lambda' \in \mathcal{O}$ is free*

The set of free operations describes channels that can be (easily) implemented under given, physical or practical constraints. The first condition in Def. 7.1 says that the identity map is free, as in most resource theories "doing nothing" is for free. Condition two says that performing free maps consecutively is free, which ensures that operations in $\mathcal{O}$ can be performed freely any number of times and in any order. These two conditions can be understood as minimal requirements for free operations. Many results on general QRTs require more assumptions, for example [CG19]:

1. $\mathcal{O}$ admits a tensor product structure: i) applying free maps to a part of a composite system is free ii) appending free states is a free operation iii) discarding a system is a free operation.
2. $\mathcal{O}$ is selectively free: free operations admit a decomposition into free Kraus operators. This ensures that the map is also free when a particular outcome of the channel is selected.
3. $\mathcal{O}$ is dually free: the (normalized) adjoint map of any free map is free. This means that the map can neither create nor detect the resource.
4. $\mathcal{O}$ is physically implementable: free operations can be generated by a sequence of free global unitaries, free measurements, and free processing of classical outcomes (free Stinespring dilation).

We discuss these properties for the resource theory of coherence in the next chapter. First, we describe quantum states that are free of the resource.

Definition 7.2 (Resource-free states)**.** *Let $\mathcal{O}$ be a set of free operations and let $\mathcal{F} \subseteq \mathrm{S}(\mathcal{H})$ be a nonempty set of quantum states. We call $\mathcal{F}$ a set of free states if for all free operations $\Lambda \in \mathcal{O}$ it holds that*

$$\Lambda[\mathcal{F}] \subseteq \mathcal{F}. \tag{7.1}$$

In other words, a set of free states is closed under all free operations. We call a state $\rho \in \mathrm{S}(\mathcal{H})\backslash\mathcal{F}$ a *resource state*. The restriction on $\mathcal{F}$ in Eq. (7.1) ensures that free operations cannot create resource from any free state. The pair $(\mathcal{F}, \mathcal{O})$ can be understood as the definition of a QRT. Such a theory can become trivial if almost any quantum operation is free and thus almost no state is resourceful, e.g., in the case $\mathcal{F} = \mathrm{S}(\mathcal{H})$. A QRT $(\mathcal{F}, \mathcal{O})$ is called convex if $\mathcal{O}$ and $\mathcal{F}$ are convex sets.

One example for a consistent set of free states is the set $\mathcal{F}_{\text{prep}}$ [CG19]. Its elements $\sigma \in \mathcal{F}_{\text{prep}}$ have the property that for any state $\rho \in \mathrm{S}(\mathcal{H})$ there exists a free operation Λ such that $\Lambda[\rho] = \sigma$. In other words, the states in $\mathcal{F}_{\text{prep}}$ can be created from "anything" (any state) without cost. The set $\mathcal{F}_{\text{prep}}$ is usually the smallest free set of interest, although it is not necessarily the smallest possible set given our definitions. This is because in principle any fixed point of the set $\mathcal{O}$ (often but not necessarily the maximally mixed state) defines the smallest possible nonempty set $\mathcal{F}$.

One can also build a QRT starting from free states. Given a subset $\mathcal{F} \subseteq \mathrm{S}(\mathcal{H})$ of quantum states, we can define $\mathcal{O}$ as a (maximal) set of operations under which $\mathcal{F}$ is closed.

Definition 7.3 (Maximally free operations)**.** *Given a subset $\mathcal{F} \subseteq \mathrm{S}(\mathcal{H})$ we define the set of maximally free operations $\mathcal{O}_{\max}$ as the set of all channels satisfying*

$$\Lambda[\mathcal{F}] \subseteq \mathcal{F}. \tag{7.2}$$

Because of Defs. 7.1 and 7.2 it is clear that $\mathcal{O}_{\max}$ corresponds to the largest set of free operations consistent with $\mathcal{F}$. The set $\mathcal{O}_{\max}$ is convex if and only if $\mathcal{F}$ is convex [CG19].

7.2 Resource Theory of Coherence

Quantum coherence describes the possibility for a quantum system to be in a superposition of different states [SAP17]. This feature, together with the measurement postulate, can be understood as the most fundamental property which differentiates quantum mechanics from the classical realm. In the history of physics,

coherence was identified as the reason for the particle-wave duality which led to the invention of quantum mechanics. Moreover, coherence underlies other phenomena such as quantum interference and quantum entanglement, which play a central role in quantum information technologies today.

In the context of quantum information, it is natural to perceive quantum coherence as a resource. Indeed, quantum information technologies often suffer from the loss of coherence (decoherence) in a particular basis, distinguished, for example, by the Hamiltonian of the system. Since coherence underlies other quantum phenomena, it is a valuable prerequisite to obtain an advantage of quantum information technologies compared to classical resources. For instance, in quantum thermodynamics, coherence in the energy eigenbasis can be utilized to extract work from a system without affecting the classical energy statistics [KJJ+18]. In quantum metrology, the estimation of a magnetic field in a certain direction requires coherence [SAP17].

Given a d-dimensional Hilbert space $\mathcal{H}$, we denote its distinguished orthonormal reference basis by $\{|i\rangle\}$. We call a state $\rho_{\mathrm{I}} \in \mathrm{S}(\mathcal{H})$ *incoherent* if it is diagonal in the reference basis, i.e., it has the form

$$\rho_{\mathrm{I}} = \sum_i p_i |i\rangle\langle i|, \tag{7.3}$$

where $\{p_i\}$ is a probability distribution. The incoherent states form a convex set $\mathcal{I} \subset \mathrm{S}(\mathcal{H})$ of free states $\mathcal{F} = \mathcal{I}$. An important feature of coherence theory is that it can be characterized by a *resource destroying map* [LHL17], namely the dephasing channel $\Delta : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H})$ given by

$$\Delta[\rho] = \sum_i \langle i|\rho|i\rangle |i\rangle\langle i|. \tag{7.4}$$

The set $\mathcal{I}$ is the image of Δ applied to the set of quantum states, $\mathcal{I} = \Delta[\mathrm{S}(\mathcal{H})]$. Moreover, the incoherent states can be characterized as the fixed points of the dephasing map, $\Delta[\rho] = \rho \Leftrightarrow \rho \in \mathcal{I}$.

7.2.1 Incoherent Operations

The set of free operations for the resource theory of coherence is not unique. Depending on the application, different classes are studied in the literature, partially inspired by the properties 2.–4. from the previous section [SAP17]. Here, we present the four most relevant classes for the purpose of this thesis and briefly discuss their properties and relations among them. We start with the largest set, the *maximally incoherent operations* (MIO), which contains all channels $\Lambda \colon \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H})$ such that

$$\Lambda[\mathcal{I}] \subseteq \mathcal{I}. \tag{7.5}$$

In other words, the class MIO corresponds to the set of maximally free operations $\mathcal{O}_{\max}$ from the previous section for the choice $\mathcal{F} = \mathcal{I}$. MIO channels can equivalently be characterized by the property [Å06]

$$\Lambda \circ \Delta = \Delta \circ \Lambda \circ \Delta. \tag{7.6}$$

The definition of incoherent maps can be readily adapted to Kraus operators. Given a set of Kraus operators $\{K_n\}$ fulfilling normalization $\sum_n K_n^\dagger K_n = \mathbb{1}$, we call K_n incoherent if

$$K_n|i\rangle \propto |j\rangle. \tag{7.7}$$

This condition is equivalent to $K_n = \sum_i c_{n,i}|f(i)\rangle\langle i|$, where $c_{n,i} \in \mathbb{C}$ and f is an index function. In particular, this includes *incoherent unitaries* which admit the form $U = \sum_i e^{i\alpha_i}|\pi(i)\rangle\langle i|$, with $\alpha_i \in \mathbb{R}$ and where π is an index permutation.

Interestingly, there are MIO maps which admit a Kraus decomposition where each Kraus operators is (maximally) coherent [SKW+18]: let $\{|n_+\rangle\}$ be a mutually unbiased basis with respect to the incoherent basis $\{|i\rangle\}$, i.e., $|\langle i|n_+\rangle|^2 = \frac{1}{d}$. Consider the Kraus operators $K_n = |n_+\rangle\langle n_+|$ which are not incoherent as they map to a coherent state. However, the channel $\Lambda[\rho] = \sum_n K_n \rho K_n^\dagger$ is in MIO since it maps any incoherent state $\sigma = \sum_i p_i|i\rangle\langle i|$ to the maximally mixed state, $\Lambda[\sigma] = \sum_n K_n \sigma K_n^\dagger = \frac{1}{d}\sum_i p_i \sum_n |n_+\rangle\langle n_+| = \frac{\mathbb{1}}{d}$.

For this reason, one introduces the class of *incoherent operations* (IO) [BCP14]. A channel Λ is in IO if there exists a Kraus decomposition $\Lambda[\rho] = \sum_l K_n \rho K_n^\dagger$ where all K_n are incoherent. This means that IO channels cannot even probabilistically create coherence: there is a Kraus decomposition such that each Kraus arm is incoherent, i.e., for all $\rho \in \mathcal{I}$ it holds that $K_n \rho K_n^\dagger / \mathrm{tr}(K_n \rho K_n^\dagger) \in \mathcal{I}$. However, note that in general it is hard to decide whether a channel is in IO, since it may be necessary to check all possible Kraus decompositions. The incoherent operations are strictly included in the maximal set, IO $\subset$ MIO [SAP17].

At last, we mention two further classes of incoherent operations. *Dephasing-covariant incoherent operations* (DIO) have the property that they commute with the dephasing operation, $\Lambda \circ \Delta = \Delta \circ \Lambda$ [CG16b, MS16]. This implies that these operations can neither create nor *detect* coherence [TEZP19]. The latter property is characterized by the condition $\Delta \circ \Lambda = \Delta \circ \Lambda \circ \Delta$, i.e., the incoherent part of the channel output is independent of the coherent part of the input. Finally, *strictly incoherent operations* are those IO maps for which each Kraus operator cannot detect coherence. Equivalently, SIO can be characterized as those operations which have an incoherent Kraus decomposition $\{K_n\}$ such that their adjoints $K_n^\dagger$ are also incoherent [WY16]. Therefore, it holds that SIO $\subset$ DIO $\subset$ MIO and SIO $\subset$ IO.

7.2.2 Golden Unit of Coherence

The resource theory of coherence has a *golden unit*, i.e., there are quantum states from which any other state can be prepared deterministically via free operations [BCP14]. As we will see in the next section, these states have necessarily maximal coherence. The canonical *maximally coherent state* is given by

$$|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle. \tag{7.8}$$

Any quantum state ρ can be prepared from $|\Psi_d\rangle$ by using incoherent operations (IO). Let $\{K_n\}_{n=1}^{d}$ be a set of operators defined as

$$K_n = \sum_{i=1}^{d} c_i |i\rangle\langle i \oplus n|, \tag{7.9}$$

with $c_i \in \mathbb{C}$ such that $\sum_i |c_i|^2 = 1$, and where $\oplus$ is the sum modulo 2. These are Kraus operators since they satisfy normalization, $\sum_n K_n^\dagger K_n = \mathbb{1}$. Moreover, all K_n are incoherent because for any incoherent state vector it holds that $K_n|i \oplus n\rangle = c_i|i\rangle$. The operators are even strictly incoherent as $K_n^\dagger$ is incoherent as well. Finally, for the maximally coherent state $|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_i |i \oplus n\rangle$, we obtain

$$K_n|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_i K_n|i \oplus n\rangle = \frac{1}{\sqrt{d}} \sum_i c_i|i\rangle. \tag{7.10}$$

Hence, any pure state $|\psi\rangle = \sum_i c_i|i\rangle$ can be prepared deterministically by the SIO map $\Lambda[\rho] = \sum_n K_n \rho K_n^\dagger$. Therefore, any state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ can be obtained from $|\Psi_d\rangle$ by an incoherent map, namely by preparing the eigenstate $|\psi_i\rangle$ with probability p_i. Lastly, we note that the full set of maximally coherent states is obtained as the orbit of $|\Psi_d\rangle$ under all incoherent unitaries [BD15].

7.2.3 Coherence Quantification

The coherence content of quantum states is quantified by suitable *coherence measures* [SAP17]. As the usefulness of a particular resource measure depends on the application, it has been proven useful to employ an axiomatic approach, that is, to demand properties that a proper coherence measure needs to satisfy. We call a real-valued function $C : \mathrm{S}(\mathcal{H}) \to \mathbb{R}$ coherence measure if:

(C1) *Faithfulness:* $C(\rho) \geq 0$ with equality if and only if $\rho \in \mathcal{I}$.

(C2) *Monotonicity:* C does not increase under incoherent operations, i.e.,

$$C(\Lambda[\rho]) \leq C(\rho) \tag{7.11}$$

for a given set of incoherent operations $\{\Lambda\}$.

(C3) *Convexity:* mixing does not increase coherence, i.e.,

$$C(\rho) \leq \sum_i p_i C(\rho_i) \tag{7.12}$$

for any convex decomposition $\rho = \sum_i p_i \rho_i$ with $\rho_i \in \mathrm{S}(\mathcal{H})$.

Note, that the coherence measure implicitly depends on the chosen incoherent basis. The conditions (C1) and (C2) can be seen as minimal requirements for a sensible measure of coherence. Condition (C3) describes the intuition that "losing information" should not increase coherence. Instead of condition (C2) a stronger condition is often employed in the literature.

(C4) *Strong Monotonicity:* C does not increase on average under selective incoherent operations, i.e.,

$$\sum_l p_l C(\rho_l) \leq C(\rho) \tag{7.13}$$

for any set of incoherent Kraus operators K_l defining probabilities $p_l = \mathrm{tr}(K_l \rho K_l^\dagger)$ and post-measurement states $\rho_l = K_l \rho K_l^\dagger / p_l$.

This condition is indeed stronger than monotonicity, because (C3) and (C4) together imply condition (C2) for the set IO [BCP14].

The standard example for a coherence measure is the *ℓ_1-norm of coherence* [BCP14], defined as

$$C_{\ell_1}(\rho) = \sum_{i \neq j} |\rho_{i,j}|, \tag{7.14}$$

where $\rho_{i,j} = \langle i|\rho|j\rangle$ are the matrix elements of ρ in the incoherent basis. This measure captures the intuition that the magnitude of the off-diagonal elements $\rho_{i \neq j}$ quantifies the coherence content of states. In particular, $C_{\ell_1}(\rho)$ satisfies (C1), (C3), (C4), as well as (C2) for the class IO [BCP14]. However, for $d \geq 3$, C_{ℓ_1} violates monotonicity (C2) for the classes MIO and DIO [BX17].

Of fundamental importance is the *relative entropy of coherence* defined as [BCP14]

$$C_{\mathrm{rel}}(\rho) = \min_{\sigma \in \mathcal{I}} S(\rho||\sigma), \tag{7.15}$$

where $S(\rho||\sigma) = \mathrm{tr}(\rho \log \rho - \rho \log \sigma)$ denotes the quantum relative entropy. The relative entropy of coherence satisfies (C1)–(C3) for the set MIO, as well as (C4). Remarkably, this measure is also one of the simplest, because it can be written as [Å06]

$$C_{\mathrm{rel}}(\rho) = S(\Delta[\rho]) - S(\rho), \tag{7.16}$$

with the dephasing operator Δ, and where $S(\rho) = -S(\rho||\mathbb{1})$ is the von Neumann entropy from Eq. (6.6). The relative entropy of coherence has several important operational meanings regarding the asymptotic interconversion of resources. We make the following definitions without giving the precise mathematical expressions which can be found in [WY16].

- The *distillable coherence* $C_{\mathrm{d}}(\rho)$ is the maximal rate $\frac{k}{n}$, at which k copies of the qubit golden unit $|\Psi_2\rangle$ can be obtained from n copies of ρ via incoherent operations in the asymptotic limit $n \to \infty$.
- The *coherence cost* $C_{\mathrm{c}}(\rho)$ is the minimal rate $\frac{k}{n}$, at which k copies of the qubit golden unit $|\Psi_2\rangle$ can be transformed to n copies of ρ via incoherent operations in the asymptotic limit $n \to \infty$.

It holds that $C_{\mathrm{d}}(\rho) \leq C_{\mathrm{c}}(\rho)$ with equality for pure states and both quantities are coherence measures satisfying (C1)–(C4) for the class MIO. Remarkably, the distillable coherence is equal to the relative entropy of coherence C_{rel} under the classes IO and MIO [WY16]. Moreover, C_{rel} also coincides with the coherence cost under MIO. This means that under the maximal set of free operations, coherence theory is reversible, i.e., $C_{\mathrm{d}}(\rho) = C_{\mathrm{c}}(\rho)$ holds for any quantum state. Coherence theory under IO is irreversible, but there is no "bound coherence", that is, $C_{\mathrm{d}}(\rho) = 0 \Leftrightarrow C_{\mathrm{c}}(\rho) = 0$ [WY16]. A recent result shows that under the class SIO bound coherence is generic: almost every mixed quantum state is undistillable, $C_{\mathrm{d}}(\rho) = 0$ [ZLY+19, LRA19]. This is particularly surprising as SIO has exactly the same conversion power as IO in pure-to-pure state transformations [CG16a].

7.3 Resource Theory of Block Coherence

The notion of quantum state coherence has been generalized in several directions. A straightforward generalization consists of relaxing the orthogonality requirement of the incoherent basis. The *resource theory of superposition* is formulated via a reference basis $\{|c_i\rangle\}_{i=1}^{d}$ of $\mathcal{H}$ that is not necessarily orthogonal [TKEP17, TVKJ17, DMR+17]. Given such a basis, free states and free operations are defined similarly to the resource theory of coherence. Also several measures can be readily generalized such that they describe the degree of superposition of quantum states with respect to the reference basis. In particular, the relative-entropy-based measure is a proper superposition measure. However, in the case of a nonorthogonal basis, the loss of symmetry also implies that particular structure of the theory is lost: i) for qubit systems there exists only a single state with maximal superposition ii) for higher dimensions, there exists no state with maximal superposition in general [TKEP17]. The QRT of superposition can be used to quantify the nonclassicality in the superposition of a finite number of optical coherent states [Gla63].

This is not possible using standard coherence theory since the optical coherent states are not orthogonal.

In this thesis, we focus on a further generalized notion of coherence which was introduced in Ref. [Å06]. This work aimed at quantifying the degree of superposition in quantum states with respect to an orthogonal decomposition of the underlying Hilbert space. We refer to this framework as the QRT of block coherence since it contains standard coherence theory as a special case and has an analog structure (see below). Although Ref. [Å06] put forward the first work on the axiomatic quantification of coherence, the QRT of block coherence is far less developed than standard coherence theory. However, we note that parts of block-coherence theory can be viewed as a special case of the QRT of asymmetry [PCB+16].

We consider a Hilbert space $\mathcal{H} = \oplus_i \pi_i$ that is partitioned into orthogonal subspaces π_i, that is, $\pi_i \perp \pi_{j\neq i}$. By denoting the projector onto the i-th subspace by P_i, the set $\boldsymbol{P} = \{P_i\}$ is a projective measurement on $\mathcal{H}$. We define *block-incoherent* (BI) states as density matrices of the form [Å06]

$$\rho_{\mathrm{BI}} = \sum_i P_i \sigma P_i, \quad \sigma \in \mathrm{S}(\mathcal{H}). \tag{7.17}$$

The resource-destroying map is now the block-dephasing operation $\Delta[\sigma] = \sum_i P_i \sigma P_i$, which sets all entries except the blocks on the diagonal to zero. Hence, the set of block-incoherent states is given by $\mathcal{I} = \Delta[\mathrm{S}(\mathcal{H})]$. In other words, block-incoherent states are block-diagonal and thus do not possess "outer" coherence across the subspaces π_i.

In the QRT of block coherence, $\mathcal{O}_{\max}$ is called the set of (maximally) block-incoherent (MBI) operations. The set MBI contains all channels satisfying

$$\Lambda_{\mathrm{MBI}}[\mathcal{I}] \subseteq \mathcal{I}, \quad \text{or equivalently,} \tag{7.18}$$

$$\Lambda_{\mathrm{MBI}} \circ \Delta = \Delta \circ \Lambda_{\mathrm{MBI}} \circ \Delta. \tag{7.19}$$

In the QRT of asymmetry, the free operations studied in the literature are the group-covariant operations, i.e., channels that commute with all unitary channels obtained from the symmetry group. In the language of coherence theory these operations are the translationally-invariant operations TIO [MSZ16], which form a strict subset of the maximal set of free operations MBI [MS16].

Block-coherence measures can be introduced in analogy to coherence measures. Given a projective measurement $\boldsymbol{P}$, we call a real-valued function $C(\cdot, \boldsymbol{P}) : \mathrm{S}(\mathcal{H}) \to \mathbb{R}$ a block-coherence measure if it satisfies the properties (C1)–(C3) from Sec. 7.2.3 for the class MBI. For that, we replace incoherent by block-incoherent and view $\mathcal{I}$ as the set of block-incoherent states. By employing condition (C2) it can be shown that any block-coherence measures $C(\rho, \boldsymbol{P})$ obeys the natural property of *block-unitary invariance*: C is invariant under unitaries acting on the subspaces

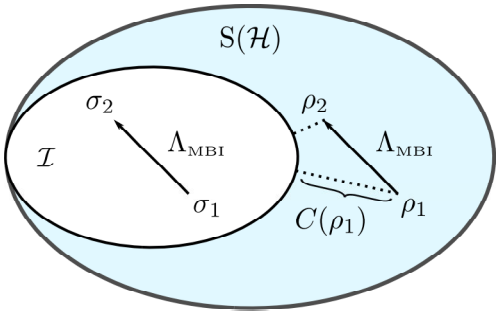

Figure 7.1: Visualization of the structure of convex quantum resource theories in the case of block coherence. The block-coherence content $C(\rho_1) \equiv C(\rho_1, \boldsymbol{P})$ of a quantum state $\rho_1 \in \mathrm{S}(\mathcal{H})$ is the distance of this state to the set $\mathcal{I}$ of block-incoherent states. Block-incoherent operations Λ_{MBI} map any state $\sigma_1 \in \mathcal{I}$ to a state $\sigma_2 \in \mathcal{I}$. When applied to a resourceful state ρ_1, the free map Λ_{MBI} decreases the distance to the set $\mathcal{I}$: with $\rho_2 = \Lambda_{\mathrm{MBI}}[\rho_1]$ it holds that $C(\rho_2) \leq C(\rho_1)$.

$\pi_i = \mathrm{im}\, P_i$ [BKB18]. The structure of the QRT of block coherence is visualized in Fig. 7.1.

Several block-coherence quantifier were introduced in [Å06] and the monotonicity condition (C2) was proven for some of them. Further block-coherence measures were presented in [BKB19]. In Ref. [BKB18] the general class of distance-based block-coherence quantifiers was investigated. We call a realvalued positive function $D(\rho, \sigma) \geq 0$ a *distance measure* on quantum states ρ, σ if $D(\rho, \sigma) = 0$ is equivalent to $\rho = \sigma$. If D additionally satisfies symmetry and the triangle inequality, it is called a metric [NC00]. For any distance D we obtain a coherence quantifier given by

$$C_D(\rho, \boldsymbol{P}) \coloneqq \inf_{\sigma \in \mathcal{I}} D(\rho, \sigma), \tag{7.20}$$

where the infimum is taken over the set of block-incoherent states. This definition immediately implies that C_D satisfies property (C1). Moreover, $C_D(\rho, \boldsymbol{P})$ from Eq. (7.20) satisfies:

- (C2) if D is contractive under any quantum operation Λ, i.e.,

$$D(\Lambda[\rho], \Lambda[\sigma]) \leq D(\rho, \sigma), \tag{7.21}$$

- (C3) if the corresponding distance is jointly convex, i.e.,

$$D(\sum_i p_i \rho_i, \sum_j p_j \sigma_j) \leq \sum_i p_i D(\rho_i, \sigma_i) \tag{7.22}$$

  holds for any ensembles $\{p_i, \rho_i\}$, $\{p_i, \sigma_i\}$ [BCP14].

It is apparent that the QRT of block coherence reduces to standard coherence theory in the special case when all effects P_i have rank one, i.e., $P_i = |i\rangle\langle i|$. Block-coherence theory has the merit that it naturally views coherence as a quantity that is defined with respect to a (projective) measurement. The next section addresses and answers the question whether the QRT of quantum coherence can also be defined with respect to the most general quantum measurement.

7.4 Resource Theory of POVM-based Coherence

In this section, we describe the broadest generalization of the QRT of coherence that currently exists: the resource theory of POVM-based coherence. Coherence is an intrinsic property of quantum states and thus should be defined with respect to general quantum measurements (POVMs). This is because POVMs describe the most general type of quantum observable, see Sec. 3.2. Moreover, POVMs can outperform projective measurements for many tasks in quantum information theory [OGWA17]. This includes quantum tomography [RBKSC04], unambiguous discrimination of quantum states [Ber10], quantum cryptography [Ben92, Ren04], Bell inequalities [Gis96, VB10] or quantum randomness generation [APVW16, BKB17].

We argued in Ref. [BKB19] that a notion of *coherence with respect to a general quantum measurement* is meaningful if: i) it can be embedded in a consistent resource theory ii) POVM-based coherence measures have interesting operational interpretations, i.e, they quantify the advantage of states in a quantum information protocol. Both points were addressed in [BKB18, BKB19], where a QRT of quantum state coherence with respect to an arbitrary POVM was introduced and studied. The content of this section is a summary of the results contained in these two manuscripts. The original publications and my precise contribution to these works can be found in App. A.2 and App. A.3. We expect that our findings will help to clarify the role of coherence in all information technologies employing nonprojective quantum measurements.

7.4.1 Summary of Results

Let $\boldsymbol{E}$ be a POVM on $\mathcal{H}$ with $d = \dim \mathcal{H}$. POVM-based coherence theory is defined by linking it to the resource theory of block coherence specified by the *Naimark extension* $\boldsymbol{P}$ of $\boldsymbol{E}$. See Sec. 4.3 to find a detailed construction of two different Naimark extensions for any POVM. In particular, we specify the minimal dimension $d' \geq d$ of the Naimark space $\mathcal{H}'$. We denote by $\mathcal{E} : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ the isometric Naimark embedding channel. It holds that

$$\mathrm{tr}(E_i \rho) = \mathrm{tr}(P_i \mathcal{E}[\rho]), \quad \text{for all } \rho \in \mathrm{S}(\mathcal{H}). \tag{7.23}$$

Hence, the Naimark extension $\boldsymbol{P}$ leads to the same expecation values for embedded states $\mathcal{E}[\rho]$ as the original POVM $\boldsymbol{E}$ for ρ. Therefore, it is natural to define the coherence of a state ρ w.r.t. a POVM $\boldsymbol{E}$ as the block coherence of $\mathcal{E}[\rho]$ w.r.t. the Naimark extension $\boldsymbol{P}$ of $\boldsymbol{E}$, namely

$$C(\rho, \boldsymbol{E}) \coloneqq C(\mathcal{E}[\rho], \boldsymbol{P}), \tag{7.24}$$

where the function C on the right denotes any block-coherence measure [BKB18]. This concept is visualized in Fig. 7.2. Since the Naimark extension of a POVM is not unique, one should ensure that the right side of Eq. (7.24) does not depend on the choice of Naimark extension $\boldsymbol{P}$. If this holds, it implies that in the special case of $\boldsymbol{E}$ being a von Neumann measurement $E_i = |i\rangle\langle i|$, that $C(\rho, \boldsymbol{E})$ generalizes the corresponding standard coherence measure [BKB19].

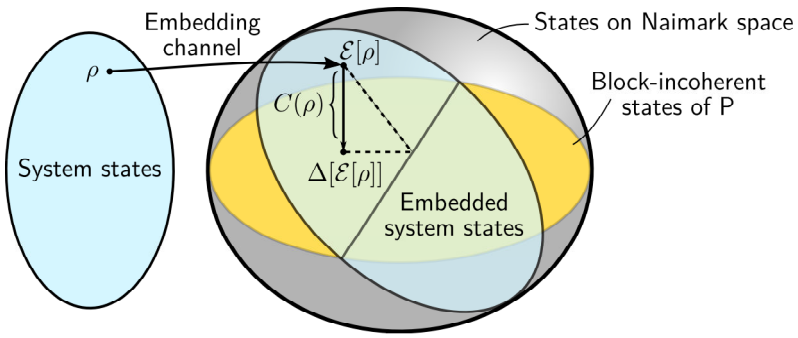

Figure 7.2: The QRT of POVM-based coherence is defined by making use of the Naimark construction. Quantum states ρ are embedded as $\mathcal{E}[\rho]$ to act on a higher-dimensional Hilbert space (Naimark space). The POVM $\boldsymbol{E}$ is extended to a projective measurement $\boldsymbol{P}$ on the Naimark space which defines a set of block-incoherent states $\mathcal{I}$. The POVM-coherence measure $C_{\mathrm{rel}}(\rho, \boldsymbol{E})$ is the distance between $\mathcal{E}[\rho]$ and its projection $\Delta[\mathcal{E}[\rho]]$ onto block-incoherent states. This figure is taken from my publication [BKB18].

The definition in Eq. (7.24) allows to characterize the states with zero coherence (POVM-incoherent states ρ_{PI}) by a simple condition [BKB18]. This can be used to show that for some POVMs the set of POVM-incoherent states is empty. The generalization of incoherent states are states with *minimal* coherence ρ_{min}, which form a set $\mathcal{M}$ that has similar properties as the standard incoherent set: it is nonempty, convex, and closed under POVM-incoherent operations, which are defined below [BKB18].

In the QRT of POVM-based coherence, free (POVM-incoherent) operations can be derived from block-incoherent operations on the enlarged space. Let Λ'_{MBI} be a block-incoherent map on states $\rho' \in \mathrm{S}(\mathcal{H}')$ on the Naimark space with the additional property that the set of embedded states $\{\mathcal{E}[\rho] \in \mathrm{S}(\mathcal{H}') : \rho \in \mathrm{S}(\mathcal{H})\}$ is closed under Λ'_{MBI}. Then, the following channel is called a POVM-incoherent

operation [BKB18]:

$$\Lambda_{\mathrm{MPI}}[\rho] = \mathcal{E}^{-1} \circ \Lambda'_{\mathrm{MBI}} \circ \mathcal{E}[\rho]. \tag{7.25}$$

The set of *maximally POVM-incoherent operations* MPI contains all channels of the above form and is the largest class of channels that cannot create POVM-based coherence. Crucially, the set MPI is independent of the chosen Naimark extension that defines Λ'_{MBI}. This invariance property of MPI implies that, in the case of von Neumann measurements, MPI coincides with the class MIO of standard coherence theory [BKB18]. Finally, the set MPI can be characterized by a semidefinite feasibility problem (SDP) by employing the methods developed in Sec. 5.3.1. In App. B we provide the Matlab file `IsMPI.m` that evaluates whether a given channel is element of MPI. This can be used to study the interconversion of resource states in the QRT of POVM-based coherence. Combining the SDP characterization of POVM-incoherent operations together with the Fidelity SDP (Lemma 5.4) allows to determine the maximally achievable fidelity

$$F_{\max}(\rho, \sigma) = \max_{\Lambda_{\mathrm{MPI}}} F(\Lambda_{\mathrm{MPI}}[\rho], \sigma) \tag{7.26}$$

between a target state $\sigma \in \mathrm{S}(\mathcal{H})$ and $\Lambda_{\mathrm{MPI}}[\rho] \in \mathrm{S}(\mathcal{H})$ [BKB18]. A Matlab file that computes the expression from Eq. (7.26) is given as `Fmax.m` in App. B.

POVM-incoherent (PI) Kraus operators were introduced in an analogy to MPI operations [BKB19]. As in standard coherence theory, the class of *selective* POVM-incoherent operations PI can be defined via incoherent Kraus operators. Also PI operations are invariant under the choice of Naimark extension and form a subset of the maximal set, PI $\subseteq$ MPI [BKB19].

Following the axiomatic approach of coherence measures, it is natural to demand that any POVM-based coherence measure satisfies the following conditions:

(P1) *Faithfulness:* $C(\rho, \boldsymbol{E}) \geq 0$ with equality iff $\rho = \rho_{\mathrm{PI}}$.

(P2) *Monotonicity:* $C(\Lambda_{\mathrm{MPI}}[\rho], \boldsymbol{E}) \leq C(\rho, \boldsymbol{E})$ for any MPI map with respect to $\boldsymbol{E}$.

(P3) *Convexity:* $C(\rho, \boldsymbol{E})$ is convex in ρ.

(P4) *Strong Monotonicity:* $C(\rho, \boldsymbol{E})$ does not increase on average under selective POVM-incoherent operations PI, i.e.,

$$\sum_l p_l C(\rho_l, \boldsymbol{E}) \leq C(\rho, \boldsymbol{E}) \tag{7.27}$$

for any set of POVM-incoherent Kraus operators K_l defining probabilities $p_l = \mathrm{tr}(K_l \rho K_l^\dagger)$ and post-measurement states $\rho_l = K_l \rho K_l^\dagger / p_l$.

Remarkably, any POVM-coherence measure $C(\rho, \boldsymbol{E})$ (7.24) satisfies the condition (P1)–(P4) if the underlying block-coherence measure satisfies (C1)–(C4) under MBI [BKB18, BKB19]. Below, we give a list of POVM-coherence measures that were introduced and studied so far [BKB18, BKB19].

- *Relative entropy of POVM-based coherence:*

$$C_{\mathrm{rel}}(\rho, \boldsymbol{E}) = H(\{p_i(\rho)\}) + \sum_i p_i(\rho) S(\rho_i) - S(\rho), \tag{7.28}$$

  with $p_i(\rho) = \mathrm{tr}(E_i \rho)$, $\rho_i = A_i \rho A_i^\dagger / p_i$, $A_i = \sqrt{E_i}$, and the Shannon entropy H from Eq. (6.14). This function satisfies (P1)–(P4).

- *Robustness of POVM-based coherence:*

$$C_{\mathrm{rob}}(\rho, \boldsymbol{E}) = \min_{\tau \in \mathrm{S}(\mathcal{H}')} \left\{ s \geq 0 : s\tau_{i,j} = -A_i \rho A_j^\dagger \ \forall i \neq j \right\}, \tag{7.29}$$

  where $\tau = \sum_{i,j} \tau_{i,j} \otimes |i\rangle\langle j|$ and $A_i = \sqrt{E_i}$. This function satisfies (P1)–(P4).

- *ℓ_1-norm of POVM-based coherence:*

$$C_{\ell_1}(\rho, \boldsymbol{E}) = \sum_{i \neq j} ||A_i \rho A_j^\dagger||_1. \tag{7.30}$$

  This function satisfies (P1) and (P3) but not (P2) in general. It is open whether it satisfies (P4).

- *The class of distance-based quantifiers:* $C_D(\rho, \boldsymbol{E})$ is defined via Eqs. (7.24), (7.20). C_D satisfies (P1), as well as (P3) if the distance is jointly convex. If D is contractive under quantum operations, $C_D(\rho, \boldsymbol{E})$ is independent of the choice of Naimark extension and satisfies (P2). This class includes the geometric POVM-based coherence $C_{\mathrm{geo}}(\rho, \boldsymbol{E})$, and the maximum relative entropy of POVM-coherence $C_{\max}(\rho, \boldsymbol{E})$ [BKB19].

All of the quantifiers above generalize well-known and frequently used measures from standard coherence theory [SAP17]. In Ref. [BKB19] we also established relations among the first three measures which are visualized in Fig. 7.3 for the qubit trine POVM from Eq. (3.29). In App. B we provide Matlab code to compute these measures, namely the files `RelEntPBC.m`, `L1NormPBC.m` and `RobPBC.m`.

The POVM-coherence measure $C_{\mathrm{rel}}(\rho, \boldsymbol{F})$ has an important operational interpretation that we explained in Sec. 6.3: it equals the private randomness $R_{X|E}$ generated by the POVM $\boldsymbol{F}$ on the state ρ with respect to an eavesdropper E holding optimal side information about the measured state [BKB19]. Fig. 7.4 (left) shows the value of $C_{\mathrm{rel}}(\psi, \boldsymbol{E}^{\mathrm{trine}})$ for the qubit trine POVM from Eq. (3.29) and

pure qubit states ψ. Note that $\boldsymbol{E}^{\text{trine}}$ yields up to $\log(3) \approx 1.58$ private random bits per measurement, compared to maximally one random bit for qubit projective measurements. The right side of Fig. 7.4 shows the conversion fidelity $F_{\max}(\rho,\sigma)$ from Eq. (7.26) for the trine POVM when starting from an initial state with less than maximal resource.

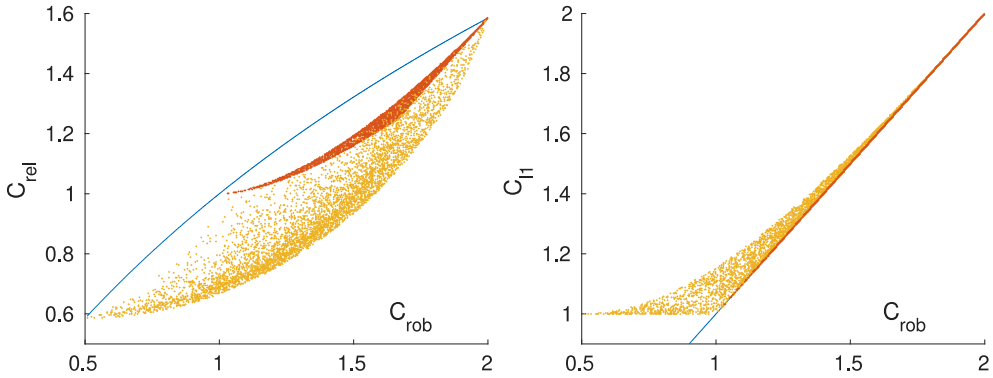

Figure 7.3: POVM-coherence measures in relation to the generalized robustness of coherence $s := C_{\text{rob}}(\rho,\boldsymbol{E})$ for the qubit trine POVM $\boldsymbol{E} = \boldsymbol{E}^{\text{trine}}$ from Eq. (3.29). *Left:* the blue line indicates the bound $C_{\text{rel}}(\rho,\boldsymbol{E}) \leq \log_2(1+s)$. Red (yellow) dots represent randomly sampled pure (mixed) states. Similar to standard coherence theory [RPWL17], the upper bound is not tight. *Right:* the blue, straight line indicates the graph of $C_{\ell_1}(\rho,\boldsymbol{E}) = s$, on which all pure states lie (red dots). The yellow dots represent mixed states for which $C_{\ell_1}(\rho,\boldsymbol{E}) \geq s$ holds. This figure is taken from my publication [BKB19].

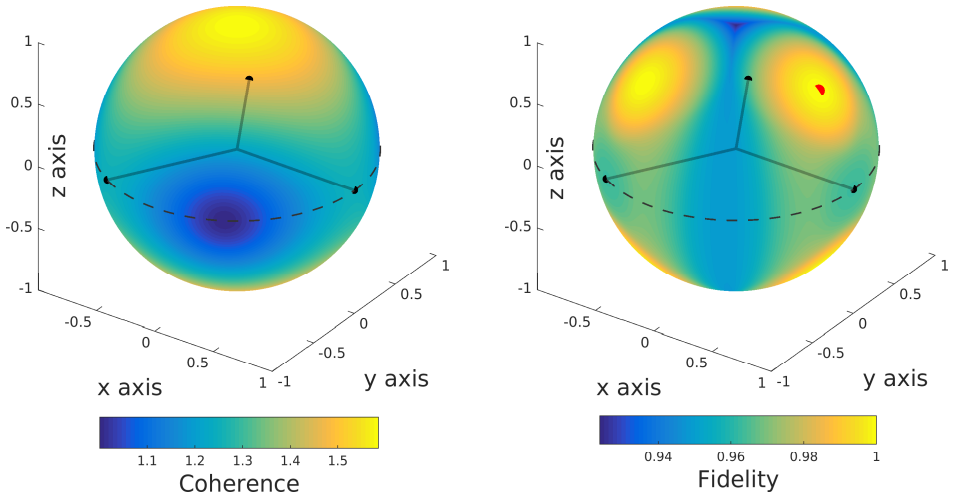

Figure 7.4: POVM-based coherence theory for qubit states with respect to the trine POVM $\boldsymbol{E}^{\text{trine}}$ from Eq. (3.29) in the Bloch sphere representation. Gray lines indicate the three measurement directions. *Left:* POVM-based coherence of pure qubits (surface of sphere). The states $|0\rangle$ and $|1\rangle$ have maximal coherence of $C = \log 3$. The Bloch vectors of the three states with the lowest pure-state coherence $C = 1$ are antipodal to the measurement directions. *Right:* Maximally achievable conversion fidelity $F_{\max}(\rho,\sigma) = \max_{\Lambda_{\text{MPI}}} F(\Lambda_{\text{MPI}}[\rho],\sigma)$ between a pure initial state ρ (red dot) subjected to POVM-incoherent operations Λ_{MPI} and a pure target state σ on the sphere surface. Here, $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle = \cos(\frac{\pi}{8})|0\rangle + \sin(\frac{\pi}{8})|1\rangle$. Only states in the orbit of $|\psi\rangle$ under the six POVM-incoherent unitaries can be reached with unit fidelity, as depicted by the yellow spots. This figure is taken from my publication [BKB18].

CHAPTER 8

Conclusion and Outlook

In this thesis, we presented results on two information-theoretical scenarios and studied the role of general quantum measurements in them.

Employing the results from my publication [BKB17], we investigated a general MDI setup for randomness generation (i.e., expansion) that consists of two devices: a source of arbitrary, well-characterized quantum states and an untrusted detector implementing any measurement. We presented a randomness generation protocol and quantified its achievable randomness gain depending on the observed measurement statistics and sent states. Our results were applied by investigating several examples of simple MDI quantum random number generators, where we outlined optimal honest strategies. In particular, we demonstrated that POVMs can yield up to twice the randomness generation rate of projective measurements. This proves the advantage of general quantum measurements over projective measurements in quantum random number generation. Our MDI setup is practical compared to fully device-independent (DI) settings, because no loophole-free Bell inequality violation is required. Moreover, our approach achieves nonzero randomness generation even for low detector qualities, whereas DI protocols abort in this scenario [PAM$^+$10]. It is possible to generalize our results by relaxing some of our assumptions. Of primary interest are adversarial attacks beyond the IID assumption and a security analysis for a finite number of rounds, which becomes relevant for devices with a low rate of raw randomness generation. Moreover, our bounds could be made tighter by establishing a bound on the single-round von Neumann entropy instead of the the single-round min-entropy.

Taking a broader perspective, we believe that in quantum randomness generation, the optimal trade-off between theoretical security and practical implementability has yet to be found. On the theoretical side, future research should identify general means to connect the many-round min-entropy to suitable single-round entropies, complementing the methods from Refs. [CFS02, Ren08, AFDF$^+$18]. The next step would consist in developing general methods to bound the single-round von Neumann entropy in partially-characterized adversarial setups, akin to the results from [ABG$^+$07].

Employing the results from my publications [BKB18, BKB19], we introduced and investigated the resource-theoretical concept of coherence with respect to a

general quantum measurement. A novel quantum resource theory was established that generalizes the popular, well-studied resource theory of quantum coherence. In particular, we proposed and analyzed several generalized resource measures. The results include a characterization of free states, free operations and resulting conversion properties within the resource theory. We found an interesting connection of POVM-based coherence to randomness generation that provides an operational meaning to the concept of coherence with respect to a measurement.

Our work provides the foundation for a full operational analysis of POVM-based coherence as a resource, similar to the results in standard coherence theory [WY16, CG16a, CG16b, YMG$^+$16]. In particular, this analysis would enable to compute the distillable POVM-coherence and the POVM-coherence cost, in analogy to [ZLY$^+$18, RFWA18, Lam19, LZ19]. As a consequence it would reveal whether our generalized resource theory is reversible under a given class of POVM-incoherent operations, or whether there exist bound resources [ZLY$^+$19, LRA19]. Future research would benefit from a possible simplification of our constructions. In particular, we believe that a purely local characterization of the POVM-incoherent operations can be obtained. Several extensions of our framework are possible. It is likely that nearly all known incoherent channel classes and coherence measures [SAP17] can be generalized to a POVM-based formulation. In addition, we expect that more POVM-based coherence measures admit an operational interpretation, which will further motivate our theory and link it to applications in quantum information science. Finally, future work could reveal the connection of POVM-based coherence to other notions of nonclassicality such as entanglement and purity [SSD$^+$15, SKW$^+$18]. We expect our advances to help clarify the role of general quantum measurements in information technologies.

Bibliography

[AAM+15] Carlos Abellán, Waldimar Amaya, Daniel Mitrani, Valerio Pruneri, and Morgan W Mitchell. Generation of fresh and pure random numbers for loophole-free bell tests. *Physical Review Letters*, 115(25):250403, 2015.

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[AF18] Rotem Arnon-Friedman. *Reductions to IID in Device-independent Quantum Information Processing*. PhD thesis, ETH Zürich, 2018.

[AFDF+18] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications*, 9(1):459, 2018.

[AFRV16] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *arXiv:1607.01797*, 2016.

[AM16] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213, 2016.

[AMVV18] Marco Avesani, Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent heterodyne-based quantum random number generator at 17 gbps. *Nature communications*, 9(1):5365, 2018.

[APVW16] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. Optimal randomness certification from one entangled bit. *Physical Review A*, 93(4):040102, 2016.

[BAK+17] Manabendra Nath Bera, Antonio Acín, Marek Kuś, Morgan W Mitchell, and Maciej Lewenstein. Randomness in quantum mechanics: philosophy, physics and technology. *Reports on Progress in Physics*, 80(12):124001, 2017.

[BCP14] T Baumgratz, M Cramer, and M B Plenio. Quantifying coherence. *Physical Review Letters*, 113(14):140401, 2014.

[BD15] Zhaofang Bai and Shuanping Du. Maximally coherent states. *Quantum Information & Computation*, 15(15&16):1355–1364, 2015.

[Bed17] Adam Bednorz. Analysis of assumptions of recent tests of local realism. *Physical Review A*, 95(4):042118, 2017.

[Ben92] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

[Ber10] János A Bergou. Discrimination of quantum states. *Journal of Modern Optics*, 57(3):160–180, 2010.

[BG15] Fernando G S L Brandão and Gilad Gour. Reversible framework for quantum resource theories. *Physical Review Letters*, 115(7):070503, 2015.

[BHO+13] Fernando G S L Brandao, Michał Horodecki, Jonathan Oppenheim, Joseph M Renes, and Robert W Spekkens. Resource theory of quantum states out of thermal equilibrium. *Physical Review Letters*, 111(25):250404, 2013.

[BKB17] Felix Bischof, Hermann Kampermann, and Dagmar Bruß. Measurement-device-independent randomness generation with arbitrary quantum states. *Physical Review A*, 95(6):062305, 2017.

[BKB18] Felix Bischof, Hermann Kampermann, and Dagmar Bruß. Resource theory of coherence based on positive-operator-valued measures. *arXiv:1812.00018*, 2018.

[BKB19] Felix Bischof, Hermann Kampermann, and Dagmar Bruß. Quantifying coherence with respect to general quantum measurements. *arXiv:1907.08574*, 2019.

[BKG+18] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556(7700):223, 2018.

[BME+16] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner. High-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *arXiv:1612.06566*, 2016.

[Bus12] Francesco Buscemi. All entangled quantum states are nonlocal. *Physical Review Letters*, 108(20):200401, 2012.

[BX17] Kaifeng Bu and Chunhe Xiong. A note on cohering power and de-cohering power. *Quantum Information & Computation*, 17(13-14):1206–1220, 2017.

[CFS02] Carlton M Caves, Christopher A Fuchs, and Rüdiger Schack. Unknown quantum states: the quantum de finetti representation. *Journal of Mathematical Physics*, 43(9):4537–4559, 2002.

[CFS16] Bob Coecke, Tobias Fritz, and Robert W Spekkens. A mathematical theory of resources. *Information and Computation*, 250:59–86, 2016.

[CG16a] Eric Chitambar and Gilad Gour. Comparison of incoherent operations and measures of coherence. *Physical Review A*, 94(5):052336, 2016.

[CG16b] Eric Chitambar and Gilad Gour. Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence. *Physical Review Letters*, 117(3):030401, 2016.

[CG19] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91(2):025001, 2019.

[CK11] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[Col09] Roger Colbeck. *Quantum and Relativistic Protocols for Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2009.

[CZM15] Z. Cao, H. Zhou, and X. Ma. Loss-tolerant measurement-device-independent quantum random number generation. *New Journal of Physics*, 17(12):125011, 2015.

[CZYM16] Zhu Cao, Hongyi Zhou, Xiao Yuan, and Xiongfeng Ma. Source-independent quantum random number generation. *Physical Review X*, 6(1):011020, 2016.

[DMR+17] Sreetama Das, Chiranjib Mukhopadhyay, Sudipto Singha Roy, Samyadeb Bhattacharya, Aditi Sen De, and Ujjwal Sen. Wave-particle duality employing quantum coherence in superposition with non-distinguishable pointers. *arXiv:1705.04343*, 2017.

[DPP05] Giacomo Mauro D'Ariano, Paoloplacido Lo Presti, and Paolo Perinotti. Classical randomness in quantum measurements. *Journal of Physics A: Mathematical and General*, 38(26):5979, 2005.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.

[Fis03] Gerd Fischer. Lineare algebra. *14. Auflage, Vieweg*, 2003.

[FRT13] Daniela Frauchiger, Renato Renner, and Matthias Troyer. True randomness from realistic quantum devices. *arXiv:1311.4547*, 2013.

[Gis96] Nicolas Gisin. Hidden quantum nonlocality revealed by local filters. *Physics Letters A*, 210(3):151–156, 1996.

[Gla63] Roy J Glauber. The quantum theory of optical coherence. *Physical Review*, 130(6):2529, 1963.

[GMDLT+13] Rodrigo Gallego, Lluis Masanes, Gonzalo De La Torre, Chirag Dhara, Leandro Aolita, and Antonio Acín. Full randomness from arbitrarily deterministic events. *Nature Communications*, 4:2654, 2013.

[GMG+18] S Gómez, A Mattar, ES Gómez, D Cavalcanti, O Jiménez Farías, A Acín, and G Lima. Experimental nonlocality-based randomness generation with nonprojective measurements. *Physical Review A*, 97(4):040102, 2018.

[GS08] Gilad Gour and Robert W Spekkens. The resource theory of quantum reference frames: manipulations and monotones. *New Journal of Physics*, 10(3):033023, 2008.

[GVW+15] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of bell's theorem with entangled photons. *Physical Review Letters*, 115(25):250401, 2015.

[HBD+15] Bas Hensen, H Bernien, AE Dréau, A Reiserer, N Kalb, MS Blok, J Ruitenberg, RFL Vermeulen, RN Schouten, C Abellán, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[Hel69] Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[HHH+03] Michał Horodecki, Karol Horodecki, Paweł Horodecki, Ryszard Horodecki, Jonathan Oppenheim, Aditi Sen De, Ujjwal Sen, et al. Local information as a resource in distributed quantum systems. *Physical Review Letters*, 90(10):100402, 2003.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009.

[HHO03] Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Reversible transformations from pure to mixed states and the unique measure of information. *Physical Review A*, 67(6):062104, 2003.

[HHP12] Erkka Haapasalo, Teiko Heinosaari, and Juha-Pekka Pellonpää. Quantum measurements on finite dimensional systems: relabeling and mixing. *Quantum Information Processing*, 11(6):1751–1763, 2012.

[Jän08] Klaus Jänich. *Lineare Algebra*. Springer, 2008.

[KAF17] Max Kessler and Rotem Arnon-Friedman. Device-independent randomness amplification and privatization. *arXiv preprint arXiv:1705.04148*, 2017.

[KJJ+18] Hyukjoon Kwon, Hyunseok Jeong, David Jennings, Benjamin Yadin, and M S Kim. Clock–work trade-off relation for coherence in quantum thermodynamics. *Physical Review Letters*, 120(15):150602, 2018.

[KRS09] Robert König, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *Information Theory, IEEE Transactions on*, 55(9):4337–4347, 2009.

[Lam19] Ludovico Lami. Completing the grand tour of asymptotic quantum coherence manipulation. *arXiv:1902.02427*, 2019.

[LBL+15] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner. Self-testing quantum random number generator. *Physical Review Letters*, 114(15):150501, 2015.

[LBS14] Yun Zhi Law, Jean-Daniel Bancal, and Valerio Scarani. Quantum randomness extraction for various levels of characterization of the devices. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424028, 2014.

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108:130503, Mar 2012.

[LHL17] Zi-Wen Liu, Xueyuan Hu, and Seth Lloyd. Resource destroying maps. *Physical Review Letters*, 118(6):060502, 2017.

[LJL+10] Thaddeus D Ladd, Fedor Jelezko, Raymond Laflamme, Yasunobu Nakamura, Christopher Monroe, and Jeremy Lloyd O'Brien. Quantum computers. *nature*, 464(7285):45, 2010.

[Löf04] J. Löfberg. Yalmip : A toolbox for modeling and optimization in matlab. In *In Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.

[LRA19] Ludovico Lami, Bartosz Regula, and Gerardo Adesso. Generic bound coherence under strictly incoherent operations. *Physical Review Letters*, 122(15):150402, 2019.

[LYW+11] Hong-Wei Li, Zhen-Qiang Yin, Yu-Chun Wu, Xu-Bo Zou, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Semi-device-independent random-number expansion without entanglement. *Physical Review A*, 84(3):034301, 2011.

[LZ19] C L Liu and D L Zhou. Deterministic coherence distillation. *Physical Review Letters*, 123(7):070402, 2019.

[LZL+18] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, et al. Device-independent quantum random-number generation. *Nature*, 562(7728):548, 2018.

[MS16] Iman Marvian and Robert W Spekkens. How to quantify coherence: Distinguishing speakable and unspeakable notions. *Physical Review A*, 94(5):052324, 2016.

[MSZ16] Iman Marvian, Robert W Spekkens, and Paolo Zanardi. Quantum speed limits, coherence, and asymmetry. *Physical Review A*, 93(5):052331, 2016.

[MVV17] Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent ultrafast quantum random number generation. *Physical Review Letters*, 118(6):060503, 2017.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NGZ+16] You-Qi Nie, Jian-Yu Guan, Hongyi Zhou, Qiang Zhang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan. Experimental measurement-device-independent quantum random number generation. *arXiv:1612.02114*, 2016.

[OGWA17] Michał Oszmaniec, Leonardo Guerini, Peter Wittek, and A Acín. Simulating positive-operator-valued measures with projective measurements. *Physical Review Letters*, 119(19):190501, 2017.

[OHdG06] B Odom, D Hanneke, B d'Urso, and G Gabrielse. New measurement of the electron magnetic moment using a one-electron quantum cyclotron. *Physical Review Letters*, 97(3):030801, 2006.

[PAM+10] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[PCB+16] Marco Piani, Marco Cianciaruso, Thomas R Bromley, Carmine Napoli, Nathaniel Johnston, and Gerardo Adesso. Robustness of asymmetry and coherence of quantum states. *Physical Review A*, 93(4):042107, 2016.

[PCSA15] Elsa Passaro, Daniel Cavalcanti, Paul Skrzypczyk, and Antonio Acín. Optimal randomness certification in the quantum steering and prepare-and-measure scenarios. *New Journal of Physics*, 17(11):113010, 2015.

[Å06] Johan Åberg. Quantifying superposition. *arXiv:quant-ph/0612146*, 2006.

[RBKSC04] Joseph M Renes, Robin Blume-Kohout, Andrew J Scott, and Carlton M Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6):2171–2180, 2004.

[Ren04] Joseph M Renes. Spherical-code key-distribution protocols for qubits. *Physical Review A*, 70(5):052314, 2004.

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[Ren13] Renato Renner. *Quantum Information Theory*. Lecture notes, February 2013.

[RFWA18] Bartosz Regula, Kun Fang, Xin Wang, and Gerardo Adesso. One-shot coherence distillation. *Physical Review Letters*, 121(1):010401, 2018.

[RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference*, pages 407–425. Springer, 2005.

[RPWL17] Swapan Rana, Preeti Parashar, Andreas Winter, and Maciej Lewenstein. Logarithmic coherence: operational interpretation of ℓ_1-norm coherence. *Physical Review A*, 96(5):052336, 2017.

[SAP17] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. Colloquium. *Reviews of Modern Physics*, 89:041003, Oct 2017.

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[Sha48] Claude Elwood Shannon. A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423, 1948.

[SKW+18] Alexander Streltsov, Hermann Kampermann, Sabine Wölk, Manuel Gessner, and Dagmar Bruß. Maximal coherence and the resource theory of purity. *New Journal of Physics*, 20(5):053058, 2018.

[SMSC+15] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical Review Letters*, 115(25):250402, 2015.

[SSD+15] Alexander Streltsov, Uttam Singh, Himadri Shekhar Dhar, Manabendra Nath Bera, and Gerardo Adesso. Measuring quantum coherence with entanglement. *Physical Review Letters*, 115(2):020403, 2015.

[TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55(12):5840–5847, 2009.

[TCR10] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min-and max-entropies. *IEEE Transactions on Information Theory*, 56(9):4674–4681, 2010.

[TEZP19] Thomas Theurer, Dario Egloff, Lijian Zhang, and Martin B Plenio. Quantifying operations with an application to coherence. *Physical Review Letters*, 122(19):190405, 2019.

[TKEP17] Thomas Theurer, Nathan Killoran, Dario Egloff, and Martin B Plenio. Resource theory of superposition. *Physical Review Letters*, 119(23):230401, 2017.

[Tom12] Marco Tomamichel. *A framework for non-asymptotic quantum information theory*. PhD thesis, ETH Zürich, 2012.

[TTT99] Kim-Chuan Toh, Michael J Todd, and Reha H Tütüncü. Sdpt3—a matlab software package for semidefinite programming, version 1.3. *Optimization methods and software*, 11(1-4):545–581, 1999.

[TVKJ17] Kok Chuan Tan, Tyler Volkoff, Hyukjoon Kwon, and Hyunseok Jeong. Quantifying the coherence between coherent states. *Physical Review Letters*, 119(19):190405, 2017.

[TYC+14] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, et al. Measurement-device-independent quantum key distribution over 200 km. *Physical Review Letters*, 113(19):190501, 2014.

[UZZ+13] Mark Um, Xiang Zhang, Junhua Zhang, Ye Wang, Yangchao Shen, D-L Deng, Lu-Ming Duan, and Kihwan Kim. Experimental certification of random numbers via quantum contextuality. *Scientific reports*, 3:1627, 2013.

[VB10] T Vértesi and E Bene. Two-qubit bell inequality for which positive operator-valued measurements are relevant. *Physical Review A*, 82(6):062115, 2010.

[Wat12] John Watrous. Simpler semidefinite programs for completely bounded norms. *arXiv:1207.5726*, 2012.

[Wat17] John Watrous. *Semidefinite Programming in Quantum Information*. Lecture notes, Winter 2017.

[WBC15] Christopher J Wood, Jacob D Biamonte, and David G Cory. Tensor networks and graphical calculus for open quantum systems. *Quantum Information & Computation*, 15:0579–0811, 2015.

[Wil13] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[Wol12] Michael M. Wolf. *Quantum Channels & Operations*. Lecture notes, July 2012.

[Wol14] Michael M. Wolf. *Quantum effects*. Lecture notes, January 2014.

[WY16] Andreas Winter and Dong Yang. Operational resource theory of coherence. *Physical Review Letters*, 116(12):120404, 2016.

[YMG+16] Benjamin Yadin, Jiajun Ma, Davide Girolami, Mile Gu, and Vlatko Vedral. Quantum processes which do not use coherence. *Physical Review X*, 6(4):041028, 2016.

[ZLY+18] Qi Zhao, Yunchao Liu, Xiao Yuan, Eric Chitambar, and Xiongfeng Ma. One-shot coherence dilution. *Physical Review Letters*, 120(7):070403, 2018.

[ZLY+19] Qi Zhao, Yunchao Liu, Xiao Yuan, Eric Chitambar, and Andreas Winter. One-shot coherence distillation: Towards completing the picture. *IEEE Transactions on Information Theory*, 1(1), 2019.

APPENDIX A

Included Publications

A.1 Measurement-device-independent randomness generation with arbitrary quantum states

Title:	Measurement-device-independent randomness generation with arbitrary quantum states
Authors:	Felix Bischof, Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review A
Impact factor:	2.907 (2018)
Date of submission:	20 March 2017
Publication status:	Published
Contribution by F.B.:	First author (input approx. 80%)

This publication corresponds to the Bibliography entry [BKB17]. A summary of the results is given in Sec. 6.4. The main framework and research objectives were devised in collaboration with my co-authors. I performed the security analysis of the general MDI randomness generation setup. Moreover, I derived the final form of the main result, the SDP in Theorem 1. The particular MDI QRNGs we investigated were devised in collaboration with my co-authors and analyzed by me. I performed all numerical computations and created the figures and plots. Finally, I prepared the manuscript and gave the bibliography concerning the state of the art.

PHYSICAL REVIEW A **95**, 062305 (2017)

Measurement-device-independent randomness generation with arbitrary quantum states

Felix Bischof,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany
(Received 20 March 2017; published 5 June 2017)

Measurements of quantum systems can be used to generate classical data that are truly unpredictable for every observer. However, this true randomness needs to be discriminated from randomness due to ignorance or lack of control of the devices. We analyze the randomness gain of a measurement-device-independent setup, consisting of a well-characterized source of quantum states and a completely uncharacterized and untrusted detector. Our framework generalizes previous schemes as arbitrary input states and arbitrary measurements can be analyzed. Our method is used to suggest simple and realistic implementations that yield high randomness generation rates of more than one random bit per qubit for detectors of sufficient quality.

DOI: 10.1103/PhysRevA.95.062305

I. INTRODUCTION

Random numbers are a fundamental resource for many information-theoretical tasks, in particular cryptography. For any task that requires secrecy, it is important that the random numbers are unpredictable for every observer, also a potential eavesdropper—a property which is called true randomness [1] or private randomness [2]. In contrast to viewing randomness as a property of actual numbers, this notion crucially depends on the process of creating the random numbers and its underlying physics. In the deterministic classical world, randomness is the result of ignorance and hence a subjective property, which cannot be proven for a powerful adversary. In nature, however, private randomness is made possible by the intrinsic unpredictability of quantum measurements: even if the whole system is known, outcomes cannot be predicted with certainty. Yet, even in quantum mechanics, true randomness cannot be certified without further assumptions. This is because realistic settings always exhibit a mixture of true quantum randomness and classical randomness. The latter may stem from uncontrolled environmental degrees of freedom but needs to be attributed to an eavesdropper's malicious tampering with the devices. The challenge consists of separating and quantifying these types of randomness while keeping the assumptions experimentally viable.

The amount of certifiable randomness depends on the level of control over the devices [3]. Device-independent (DI) randomness generation protocols [4–7] view all devices as black boxes and certify randomness via the violation of a Bell-type inequality and thus require loophole-free Bell tests. While these have recently been demonstrated experimentally [8–11], DI randomness generation setups are far from practical.

More practical schemes are obtained by introducing additional assumptions, e.g., semi-device-independent randomness generation [12–14], the quantum steering scenario [15], and others. In this work, we discuss measurement-device-independent (MDI) randomness generation, of which a particular instance was introduced in Ref. [16] and has recently been realized in experiment [17]. The MDI setup consists of two devices: a well-characterized state source and a completely uncharacterized detector. While previous work [16] provides the randomness generation rate of a specific two-outcome single-qubit setup, we introduce and analyze a general framework which encompasses all MDI randomness generation setups, with an arbitrary state source and detector. This allows us to devise practical setups that yield up to twice the randomness of the previous work [16].

This paper is structured as follows. In Sec. II we introduce the general MDI randomness generation protocol. In Sec. III we discuss the eavesdropper's degrees of freedom and state the optimization problem in terms of a semidefinite program. Finally, examples and practical applications of our result are provided in Sec. IV.

II. MEASUREMENT-DEVICE-INDEPENDENT RANDOMNESS GENERATION

A. Setup and protocol

The MDI randomness generation setup consists of two devices (see Fig. 1). The first is a source, able to emit a set of well-characterized quantum states of arbitrary (finite) dimension. In particular, for the input a the state $\rho(a)$ is sent. Second is an uncharacterized detector which announces an outcome x whenever a state was sent. The knowledge of the quantum states and the measurement results are used to characterize the detector.

We denote the user of the protocol Alice, and the adversary Eve. Alice sets up the devices in a secure laboratory which is shielded from any kind of information transfer to the outside world. It is verified that the sending box has no further degrees of freedom than to emit a quantum state upon receiving a specific input. The adversary Eve may have built the detector but has no access to the laboratory afterwards.

The sent states $\rho(a)$ are selected via an initial string of random numbers. Because of that, we describe a randomness expansion scheme [2,4]: a user with access to an initial random string $\mathbf{A} = (a_1, a_2, \dots)$ interacts roundwise with a device leading to a string $\mathbf{X} = (x_1, x_2, \dots)$, which contain the input and output of each round, respectively. The randomness expansion protocol then outputs a processed string $\tilde{\mathbf{X}}(\mathbf{X})$ which is close to uniform, conditioned on $\mathbf{A}$ as well as on any side information E previously stored in the device.

The MDI randomness expansion protocol is as follows:

(1) For every round, do steps 2 and 3.

*felix.bischof@hhu.de

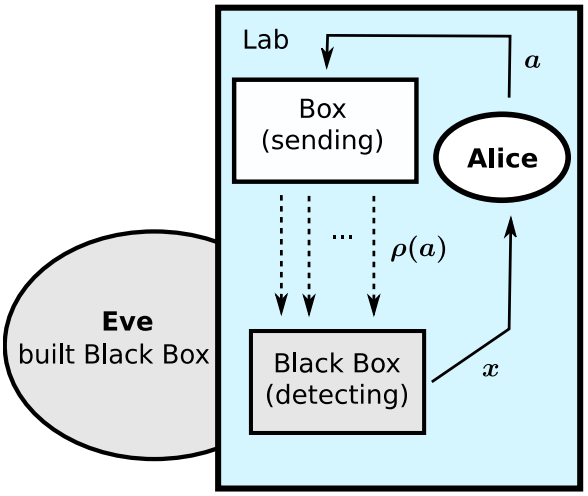

FIG. 1. The measurement-device-independent setup for randomness generation (for details see text). The trusted source sends for the input $a \in \{1, \ldots, n_s\}$ a known state $\rho(a)$ to an untrusted measurement device (black box), which outputs x with $x \in \{1, \ldots, n_o\}$. The outcome randomness $\mathcal{R}_X$ is characterized by the observed probability distribution $P_{\text{obs}}(x,a)$, i.e., the probability that the pair (x,a) occurs.

(2) The sending box sends a state $\rho(a)$ of dimension d with randomly chosen $a \in \{1, \ldots, n_s\}$ to the measurement box. On average, this uses up $\sum_a p_a(-\log_2(p_a))$ bits of the initial randomness per round, where p_a denotes the probability that $\rho(a)$ was sent.

(3) After the state $\rho(a)$ has been sent, the measurement box outputs $x \in \{1, \ldots, n_o\}$ distributed according to p_x. Potential losses can be announced as an extra no-detection outcome which is appended to the proper outcomes, or the device randomly attributes measurement results, which contributes to the noise. The only requirement is that the detector gives an outcome in *every* round.

(4) After many rounds, Alice estimates the observed measurement statistics $P_{\text{obs}}(x,a) = p_a P_{\text{obs}}(x|a)$, i.e., the probability that the pair (x,a) occurs. From that the randomness gain per round $\mathcal{R}_X$ can be computed (see below).

(5) Alice uses some further bits of the initial random string to postprocess the raw output into a shorter string of fresh private random numbers.

In the last step of the protocol, the user applies a quantum-secure extraction protocol to transform the output string $\mathbf{X}$ to a string $\tilde{\mathbf{X}}$ that is close to uniform with respect to Eve and the input. This can be done via seeded extraction, e.g., two-universal hashing, for which some further random bits are needed. For details, see Ref. [1] and references therein.

B. Randomness quantification

For the extraction protocol it is necessary to quantify the minimal number of bits needed for Eve to reconstruct the measurement result from her side information, i.e., the conditional min-entropy [18]. The single-round degrees of freedom in randomness expansion can be described by a tripartite state ρ_{XAE} on the single-round classical output and input registers and Eve's system, which reads

$$\rho_{XAE} = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_{AE}(x), \tag{1}$$

where $\{|x\rangle\}$ denotes a family of orthonormal states on X. The randomness contained in the random variable X, associated to p_x, is quantified by the conditional min-entropy

$$\mathcal{R}_X = H_{\min}(X|AE) \tag{2}$$

that measures the unpredictability of X with respect to the classical system A and the quantum system E. For *classical-quantum* states it is known [19] that the min-entropy can be expressed via the optimal guessing probability

$$H_{\min}(X|AE) = -\log_2[P^*_{\text{guess}}(X|AE)], \tag{3}$$

defined as

$$P^*_{\text{guess}}(X|AE) = \max_{\{F(x)\}} \sum_x p_x \text{tr}(F(x)\rho_{AE}(x)). \tag{4}$$

Here, $\{F(x)\}$ denotes a positive operator-valued measure (POVM) on the system AE, i.e., a collection of positive-semidefinite operators $F(x) \geqslant 0$ fulfilling $\sum_{x=1}^{n_o} F(x) = \mathbb{1}$.

III. ANALYSIS OF RANDOMNESS GENERATION

A. Eavesdropping characterization

Before introducing the degrees of freedom in the MDI setup, we list the assumptions below:

(1) The laboratory is shielded from any information transfer to the outside.

(2) The sending device's behavior is fully characterized to emit a single specific state $\rho(a)$ upon receiving the input a.

(3) The measurement device employs an independent and identically distributed (i.i.d.) strategy; i.e., it behaves independently and identically in each round.

(4) We consider the asymptotic limit; i.e., the measurement statistics is precisely known.

The first condition is necessary in any randomness expansion scheme, since otherwise the generated output could be transmitted to Eve directly. The second assumption is what differentiates MDI from fully device-independent schemes. The third condition corresponds in the language of quantum key distribution (QKD) to individual attacks. In Ref. [16], the authors describe how to prove the security of the MDI setup against collective attacks solely by employing the security proof against individual attacks and convexity arguments. If the arguments given there hold, this proof would also be applicable in our analysis, extending the result to collective attacks.[1]

Given these assumptions, the eavesdropper's most general strategy in the MDI setup is as follows. Eve has built the measurement apparatus that deviates from the honest device in two ways (see Fig. 2). First, to obtain correlations with the measurement outcome, she has hidden a system E' in the box.

[1]However, we are not sure whether the tensor product structure of the (effective) detector POVM across different rounds, employed in the proof, can be guaranteed for MDI collective attacks.

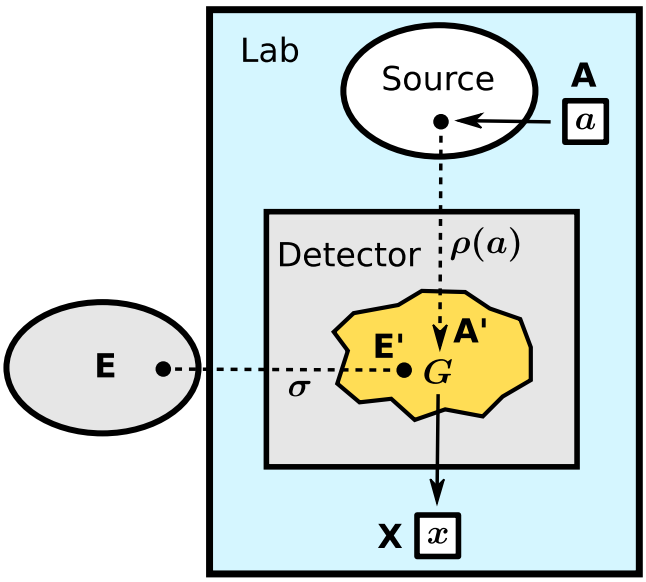

FIG. 2. The graphic depicts the relevant systems, states, and measurement to estimate the randomness generation rate, which is conditioned on the outside systems A and E. The primed systems are contained in the measurement box and represent internal degrees of freedom (E') as well as the incoming state $\rho(a)$ (A'). A further internal degree of freedom is given by the unknown measurement $\{G(x)\}$, which produces the outcome x in the laboratory. The state σ provides correlations between the detector degrees of freedom and Eve's site E.

Her distant laboratory E and the hidden system share a state σ that may contain arbitrary amounts of entanglement. Second, upon receiving the incoming states $\rho(a)$, the measurement apparatus performs an unknown measurement $\{G(x)\}$ on it and part of σ, leading to the outcome x in the laboratory. Eve aims to adjust her state and the performed measurements in such a way that she is perfectly correlated with the laboratory outcome, while producing the measurement statistics expected from the device. Furthermore, the analysis includes the correlation of the output system X with the input system A. Conditioning on the input ensures the outcome randomness to be "fresh," i.e., independent of the initial randomness.

B. Degrees of freedom in the MDI setup

In order to characterize the general way that the state in Eq. (1) is obtained in the MDI setup, we introduce the relevant systems and operators below. Each system S is associated to a Hilbert space $\mathcal{H}_S$, on which the operators act.

(1) A and X denote classical registers that store the input a and output x of each round, respectively.

(2) The incoming state $\rho(a)$ is associated to A'.

(3) Eve has equipped the measurement apparatus with an additional system E' that shares an arbitrary state σ with her site E.

(4) The measurement box performs an unknown POVM $\{G(x)\}$ with n_o outcomes on the primed system $A'E'$ whose result is stored in X.

(5) The optimal POVM from Eq. (4) on AE is denoted by $\{F(e)\}$, with $e \in \{1,\ldots,n_o\}$.

In the following, we formulate the security analysis as an optimization problem, whereby A and E try to guess X, while their operations are consistent with the classical data in the laboratory. The initial average global state reads

$$\rho_{\text{in}} = \sum_a p_a |a\rangle\langle a|_A \otimes \rho_{A'}(a) \otimes \sigma_{E'E}, \tag{5}$$

while the register X is initialized with an uncorrelated state. We denote by $\rho_{\text{in}}(a)$ the initial global state if a has occurred. The box measurement $\{G(x)\}$, which acts on $A'E'$, maps the state on AE into an ensemble $\{p_x, \tau_{AE}(x)\}$ given by

$$\tau_{AE}(x) = \frac{1}{p_x} \text{tr}_{A'E'}(G_{A'E'}(x) \otimes \mathbb{1}_{AE}\ \rho_{\text{in}}), \tag{6}$$

where tr_S denotes the partial trace over S. According to Eq. (4), these states are distinguished by a measurement $\{F(e)\}$. Its outcome $e = x$ represents the system AE's guess of the output x of the detector.

We denote the probability of the event (x,e) as $p_{x,e}$, which is given by

$$p_{x,e} = p_x \text{tr}(F_{AE}(e)\tau_{AE}(x)). \tag{7}$$

With that, the guessing probability from Eq. (4) can be formulated as $P^*_{\text{guess}}(X|AE) = \max_{\{F(x)\}} \sum_x p_{x,x}$. By combining Eqs. (6) and (7), we obtain

$$\begin{aligned} p_{x,e} &= \text{tr}_{AE}(F_{AE}(e)\ \text{tr}_{A'E'}(G_{A'E'}(x) \otimes \mathbb{1}_{AE}\ \rho_{\text{in}})) \\ &= \text{tr}(G_{A'E'}(x) \otimes F_{AE}(e)\ \rho_{\text{in}}), \end{aligned} \tag{8}$$

where in the second line we have used that, for all linear operators L_1 on $\mathcal{H}_1$, and Γ_{12} on $\mathcal{H}_1 \otimes \mathcal{H}_2$, it holds that $L_1 \text{tr}_2(\Gamma_{12}) = \text{tr}_2(L_1 \otimes \mathbb{1}\Gamma_{12})$. In Ref. [20] it was proven that when conditioning on classical information, here given by the register A, the optimal measurement in Eq. (4) consists of choosing an optimal POVM on E for each a, i.e.,

$$F_{AE}(e) = \sum_a |a\rangle\langle a|_A \otimes F_E(e|a), \tag{9}$$

where $\{F_E(e|a)\}$ is a family of POVMs on E (with outcome e), indexed by a, fulfilling

$$F_E(e|a) \geqslant 0, \quad \sum_e F_E(e|a) = \mathbb{1} \quad \forall a. \tag{10}$$

Next, we consider the action of the measurement $F_{AE}(e)$ on the initial global state $\rho_{\text{in}}(a)$ for an observer with access to A. The state after measurement on $E'E$ is given by

$$\lambda_{e|a}\sigma_{E'E}(e,a) = \text{tr}_{A'A}(\sqrt{F_{AE}(e)}\ \rho_{\text{in}}(a)\sqrt{F_{AE}(e)}^{\dagger}), \tag{11}$$

where $\lambda_{e|a}$ denotes the probability to obtain the outcome e given a, and $\sigma_{E'E}(e,a)$ is the corresponding conditional state. Note that the unitary degree of freedom of the postmeasurement state plays no role in the following, as the system E is traced out. Since Eve's outside laboratory has no access to the input, her description of the postmeasurement state is given by $\sum_a p_a \lambda_{e|a}\sigma_{E'E}(e,a)$. Note that because of the preparation by measurement, it holds that $\sigma_{E'}(e,a) = \text{tr}_E(\sigma_{E'E}(e,a))$ is independent of a, when averaged over e:

$$\sum_e \lambda_{e|a}\sigma_{E'}(e,a) = \sigma_{E'} \quad \forall a, \tag{12}$$

i.e., the index a determines a particular ensemble $\{\lambda_{e|a},\sigma_{E'}(e,a)\}$ of the state $\sigma_{E'}$. This is because a local measurement, if the outcome cannot be communicated, does not influence a remote part of a state. It is known from quantum steering that, for a suitable global state, any local state can be prepared by a measurement on the other side [21].

Altogether, we obtain

$$\begin{aligned} p_{x,e} &= \sum_a p_a p_{x,e|a} \\ &= \sum_a p_a \mathrm{tr}(G_{A'E'}(x)\rho_{A'}(a) \otimes \lambda_{e|a}\sigma_{E'}(e,a)), \end{aligned} \tag{13}$$

where only the (primed) degrees of freedom in the measurement box need to be considered.

In our protocol we observe the statistics $P_{\mathrm{obs}}(x,a)$, which constrains any valid strategy:

$$\begin{aligned} P_{\mathrm{obs}}(x,a) &= \sum_e p_a p_{x,e|a} \\ &= p_a \mathrm{tr}(G_{A'E'}(x)\rho_{A'}(a) \otimes \sigma_{E'}). \end{aligned} \tag{14}$$

Here, the average over Eve's outcomes was taken, because they are unobservable for the user, and we have used Eqs. (12) and (13) in the second line.

C. The optimization problem

We summarize the results of the previous section by stating the optimization problem for the guessing probability. Since we are left with only two subsystems in the detector $A'E'$, we omit the system subscript:

$$\begin{aligned} &P^*_{\mathrm{guess}}(X|AE) = \max_{\{G,\hat{\sigma}\}} \sum_{x,a} p_a \mathrm{tr}(G(x)\rho(a) \otimes \hat{\sigma}(x|a)) \\ &\text{such that} \quad G(x) \geqslant 0, \quad \sum_x G(x) = \mathbb{1}, \\ &\hat{\sigma}(e|a) \geqslant 0, \quad \sum_e \mathrm{tr}(\hat{\sigma}(e|a)) = 1 \quad \forall a, \\ &\sum_e \hat{\sigma}(e|a) = \sum_e \hat{\sigma}(e|1) \quad \forall a, \text{ and} \\ &P_{\mathrm{obs}}(x,a) = \sum_e p_a \mathrm{tr}(G(x)\rho(a) \otimes \hat{\sigma}(e|a)). \end{aligned} \tag{15}$$

The optimization runs over ensembles $\{\hat{\sigma}(e|a)\}$ with $\hat{\sigma}(e|a) = \lambda_{e|a}\sigma(e,a)$ of arbitrary dimension and a POVM $\{G(x)\}$ acting on it and the incoming state. The fourth line represents the requirement from Eq. (12), and the last line ensures that the detector degrees of freedom give rise to the observed probability distribution. This optimization problem is not straightforwardly feasible, as it has a nonlinear target function with linear and semidefinite constraints. However, we observe that the degrees of freedom relevant for the guessing probability can be combined into a single effective measurement acting only on the known state $\rho(a)$. For that, we define an effective measurement $M_{x,e|a}$ on $\mathcal{H}_{A'}$ via

$$M_{x,e|a} := \lambda_{e|a}\mathrm{tr}_{E'}(G_{A'E'}(x)\, \mathbb{1}_{A'} \otimes \sigma_{E'}(e,a)), \tag{16}$$

with which we can write

$$P^*_{\mathrm{guess}}(X|AE) = \sum_{x,a} p_a \mathrm{tr}(M_{x,x|a}\rho_{A'}(a)) \tag{17}$$

by comparison with Eq. (15). We instead optimize over a superset of the actual degrees of freedom relevant for the guessing probability, which consists of linear operators $M_{x,e|a}$ on $\mathcal{H}_{A'}$ with semidefinite and linear constraints that follow from Eq. (16). This, in turn, will yield an upper bound to the guessing probability and consequently a lower bound to the randomness gain. These constraints are as follows. The operator defined by Eq. (16) is positive semidefinite, since all constituents are positive semidefinite, and furthermore fulfills for all a

$$\sum_{x,e} M_{x,e|a} = \sum_x \mathrm{tr}_{E'}(G_{A'E'}(x)\mathbb{1}_{A'} \otimes \sigma_{E'}) = \mathbb{1}_{A'}, \tag{18}$$

where we have used Eq. (12) in the first equality. Thus, it has the properties of a family of POVMs on $\mathcal{H}_{A'}$, indexed by a, where the outcome x goes to Alice and e to Eve. Two further properties can be observed, which read

$$\sum_x M_{x,e|a} \propto \mathbb{1}, \tag{19}$$

$$\sum_e M_{x,e|a} = \sum_e M_{x,e|a'}, \tag{20}$$

where Eq. (19) follows directly from Eq. (16), and Eq. (20) follows from Eq. (12). Thus, strategies given by a POVM family $\{M_{x,e|a}\}$ with properties (19) and (20) include the actual strategy (15), but may not fully characterize it. The new formulation is characterized by only linear and semidefinite constraints and due to the linearity of the target function can be cast into the form of a semidefinite program (SDP).

Theorem 1. The optimal guessing probability in any MDI randomness generation setup, subject to the assumptions explained in Sec. III A, is upper bounded by the solution of the following SDP:

$$\begin{aligned} &P^*_{\mathrm{guess}}(X|AE) \leqslant \max_{\{M_{x,e|a}\}} \sum_{x,a} p_a \mathrm{tr}(M_{x,x|a}\rho(a)) \\ &\text{such that} \quad M_{x,e|a} \geqslant 0, \quad \sum_{x,e} M_{x,e|a} = \mathbb{1} \quad \forall a, \\ &\sum_x M_{x,e|a} = \left[\sum_x M_{x,e|a}\right]_{11} \cdot \mathbb{1} \quad \forall e,a, \\ &\sum_e M_{x,e|a} = \sum_e M_{x,e|1} \quad \forall x,a, \text{ and} \\ &P_{\mathrm{obs}}(x,a) = \sum_e p_a \mathrm{tr}(M_{x,e|a}\rho(a)). \end{aligned} \tag{21}$$

The second line characterizes the operators $\{M_{x,e|a}\}$ as a POVM for each a. The third and fourth lines ensure that the POVM family $\{M_{x,e|a}\}$ obeys the properties (19) and (20), respectively, which follow from the form of the effective measurement (16). The former property may be interpreted as a nonsignaling condition between the detector and Eve's site,

and the latter as a nonsignaling condition between the systems A and E. The notation $[M]_{11}$ denotes the $(1,1)$ element of the matrix M. The last line ensures that the adversary's operations actually give rise to the observed measurement statistics P_{obs} in the laboratory. The outcome of the SDP provides via Eqs. (2) and (3) a lower bound to the randomness generated per round $\mathcal{R}_X$ in the measurement-device-independent setup.

IV. RESULTS

For any MDI setup with arbitrary detector and state source, the observed probability vector can be read into the SDP (21) to determine the randomness of the output bits. In the following, we discuss which sets of states $\{\rho(a)\}$ and observed distributions $p_a P_{\text{obs}}(x|a)$ are optimal in practical setups.

Our model of the detector behavior consists of a proposed ideal quantum measurement mixed with white noise,

$$P_{\text{obs}}(x,a) = \eta P_{\text{id}}(x,a) + \frac{1-\eta}{n_o} p_a, \tag{22}$$

where P_{id} is the distribution of the ideal measurement, $\eta \in [0,1]$ is a quality parameter, n_o is the number of outcomes, and p_a is the input distribution.

In order to characterize the detector, we make use of the tomographically complete qubit state set $\{|+\rangle,|0\rangle,|1\rangle,|+i\rangle\}$, corresponding to the ± 1 eigenstates of Pauli σ_z and the $+1$ eigenstates of σ_x,σ_y. We employ pure states since we wish to minimize the input randomness.

An upper bound of the MDI randomness gain is given by the classical conditional min-entropy of the input and output distributions [20]:

$$H_{\min}(X|A) = -\log_2 \left[\sum_a \max_x P_{\text{obs}}(x,a) \right]. \tag{23}$$

In order to maximize this expression we need to have unbiased measurement outcomes x for every input a. Since for an ideal quantum measurement we cannot ensure unbiased outcomes with respect to each of the input states, we make use of an input distribution p_a that is almost sharp. This means that the first state $|+\rangle$ from the ordered list of states is sent with probability $q \equiv p_1 \to 1$, and the other states are only sent rarely to characterize the detector. We call the parameter q asymmetry of the distribution p_a. Furthermore, an asymmetric choice of inputs is desirable for randomness expansion in the asymptotic limit, as it reduces the input randomness (see step 2 of the protocol in Sec. II).

To make the limit $q \to 1$ feasible in the SDP, we divide all rounds into test and generation rounds: in test rounds, states are sent according to a uniform distribution, and in generation rounds, only $\rho(1)$ is sent. The asymptotic limit is then defined as the number of rounds $N \to \infty$. Simultaneously we take the limit $q \to 1$ to ensure maximal asymmetry. Similarly to QKD Eve's optimal strategy is now as follows: She provides a POVM that reproduces the expected measurement statistics in the *test* rounds, but aims at optimally predicting the outcomes of *generation* rounds, since test rounds have negligible contribution to the total guessing probability in the limit $q \to 1$.

In this asymmetric scenario, the optimal situation for randomness generation (expansion) corresponds to the measurement statistics of a POVM with three properties:

(i) The POVM is extremal [22]; i.e., it cannot be given as a mixture of two different POVMs [23]. This ensures that its outcomes cannot be predicted by having access to a random variable (which determines the mixing) and thus maximizes randomness with respect to the measurement apparatus controlled by Eve.

(ii) The POVM has unbiased outcomes for the first input state; i.e., the output distribution has maximal entropy.

(iii) The POVM has d^2 outcomes for the state space dimension d. This is because d^2 corresponds to the highest number of independent outcomes: any further POVM element can be written as a linear combination of previous ones, which amounts to classical postprocessing that cannot increase the true randomness. Therefore, the maximally achievable randomness is $2\log_2 d$ bits [24].

We stress that this POVM is realized in the optimal *honest* device, i.e., a device that implements a particular predefined POVM. The semidefinite program, on the other hand, finds the optimal measurement for Eve that gives rise to the measurement statistics expected from the honest device.

We have no proof of optimality of the considered Pauli-eigenstate preparations, but in the scenarios below these states perform equally well or better than randomly chosen pure states. For the considered asymmetric input distribution, where the first state has unbiased outcomes, we have found numerically (i) that the randomness gain does not depend on which set of tomographically complete states is used and (ii) for two sent states it is optimal for the second state to be an eigenstate of the measurement as this poses the strongest constraint on the classical noise of the detector.

A. Single-qubit setups

From the previous section, it follows that a qubit measurement can have up to four independent outcomes. In the following, we compare the performance in randomness gain of different sets of sent states and numbers of outcomes. In practice, the configuration is chosen by taking into account which states and measurements are most readily available in the laboratory.

In general, qubit POVM elements can be decomposed as

$$M_k = \alpha_k(\mathbb{1} + \vec{m}_k \cdot \vec{\sigma}) \quad \text{with} \quad \alpha_k > 0,$$
$$\sum_k \alpha_k = 1, \quad \sum_k \alpha_k \vec{m}_k = 0, \tag{24}$$

where $k = 1,\ldots,n_o$. To ensure unbiased measurement outcomes with respect to the most frequent state, we require

$$\langle +|M_k|+\rangle \equiv \alpha_k(1 + \vec{m}_k \cdot \vec{e}_1) = \frac{1}{n_o} \quad \forall k = 1,\ldots,n_o. \tag{25}$$

Furthermore, we have the following extremality conditions [22]. The POVM elements have rank 1, which is ensured by normalized measurement directions $|\vec{m}_k| = 1$. Additionally, the measurement operators are linearly independent. This is fulfilled, e.g., for four outcomes if and only if the measurement

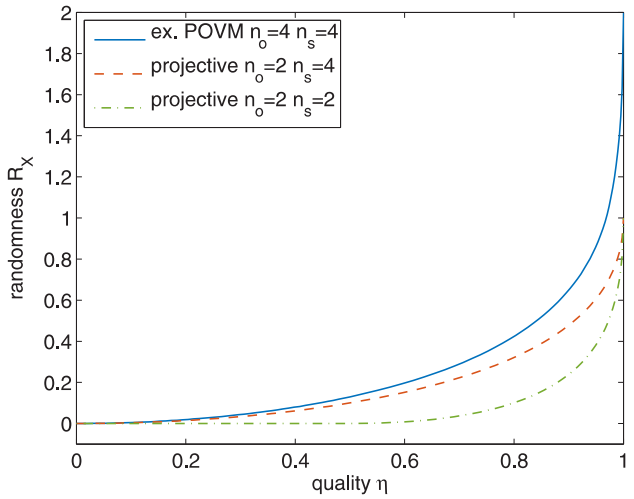

FIG. 3. The randomness rate versus the detector quality defined in Eq. (22) in the asymptotic limit and for $q \equiv p_1 \to 1$. The solid (dashed) line depicts an extremal POVM with $n_o = 4$ ($n_o = 2$) outcomes for a tomographically complete set of $n_s = 4$ states. The ideal measurement statistics arises from the measurement directions in Eq. (26) ($n_o = 4$) and from a σ_z measurement ($n_o = 2$). The lower line corresponds to the case of two nonorthogonal sent states and two outcomes.

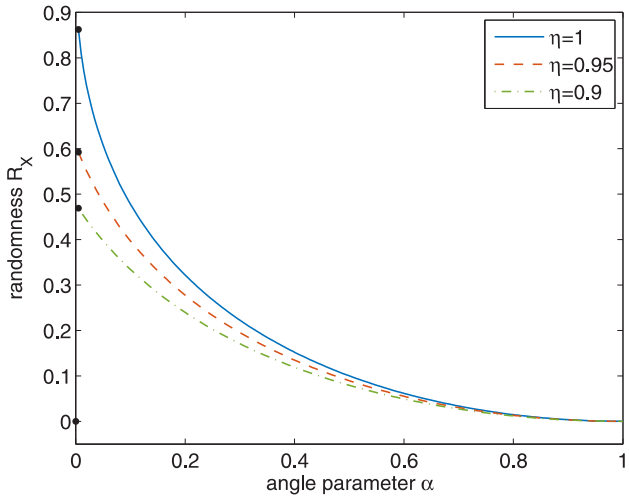

FIG. 4. The randomness rate as a function of the angle parameter α [see Eq. (28)] between two sent states for several detector qualities η and asymmetry $q = \frac{1}{2}$. The statistics of the ideal measurement corresponds to a σ_x measurement. For $\alpha = 0$, the randomness rate is equal to zero.

directions form a tetrahedron; i.e., they cannot lie in a common plane.

Note that not all α_k can be equal, since then the property (25) would force all vectors to lie in the plane defined by $\vec{m}_k \cdot \vec{e}_1 = c$, which violates the extremality condition. A maximally symmetric four-outcome configuration is given by

$$\begin{aligned} \vec{m}_1 &= \vec{e}_1, \quad \vec{m}_2 = -\frac{1}{7}\vec{e}_1 + \frac{4\sqrt{3}}{7}\vec{e}_2, \\ \vec{m}_{3/4} &= -\frac{1}{7}\vec{e}_1 - \frac{2\sqrt{3}}{7}\vec{e}_2 \pm \frac{6}{7}\vec{e}_3, \\ \alpha_1 &= \frac{1}{8}, \quad \alpha_2 = \alpha_3 = \alpha_4 = \frac{7}{24}, \end{aligned} \tag{26}$$

which we make use of in the following.

Also, we later employ a three-outcome extremal POVM given by

$$\begin{aligned} \vec{m}_1 &= \vec{e}_2, \quad \vec{m}_{2/3} = -\frac{1}{2}\vec{e}_2 \pm \frac{\sqrt{3}}{2}\vec{e}_3, \\ \alpha_1 &= \alpha_2 = \alpha_3 = \frac{1}{3}. \end{aligned} \tag{27}$$

Figure 3 compares the performance of different numbers of outcomes and sent states in the asymptotic limit as a function of the detector quality η. For $n_s = 2$ ($n_s = 4$), states are drawn from the first two (all) elements of the set $\{|+\rangle, |0\rangle, |1\rangle, |+i\rangle\}$. The measurement statistics is described by Eq. (22), where P_{id} is the distribution, which we obtain if, for $n_o = 4$, the honest device implements the four-outcome measurement (26), and for $n_o = 2$ a σ_z measurement. The optimization is performed with standard tools such as YALMIP [25], and SDPT3 [26] as solver. We observe that states drawn from a tomographically complete set in test rounds are clearly advantageous, since these allow for a better detector characterization. Moreover, the figure shows that for fixed input states, the performance of an extremal four-outcome measurement is, depending on the visibility, up to twice as good as the best projective measurement. In particular, the maximal local randomness of two bits is reached for a noiseless detector ($\eta = 1$). For a detector quality of $\eta \geqslant 97\%$, the setup generates more than one random bit per qubit. In the special case of a one-qubit sending box with tomographically complete states in the asymptotic limit, and ideal statistics given by a σ_z measurement, our bound is equal to the exact formula from previous work [16].

1. *Randomness for different relative angles*

We are also able to study the angle dependency between two states of the MDI randomness rate. Consider the case of the observed distribution (22), where P_{id} corresponds to the statistics of a σ_x measurement. For any $\alpha \in [0,1]$, the two sent states are drawn from the set $\{|\phi_\alpha\rangle, |\psi_\alpha\rangle\}$ with

$$\begin{aligned} |\phi_\alpha\rangle &= \sqrt{1 - \frac{\alpha}{2}}|0\rangle + \sqrt{\frac{\alpha}{2}}|1\rangle, \\ |\psi_\alpha\rangle &= \sqrt{1 - \frac{\alpha}{2}}|0\rangle - \sqrt{\frac{\alpha}{2}}|1\rangle. \end{aligned} \tag{28}$$

Figure 4 depicts the randomness generation rate for several detector qualities as a function of $\alpha \in [0,1]$. For $\alpha = 0$ both states are identical, $|\phi_0\rangle = |\psi_0\rangle = |0\rangle$, and for $\alpha = 1$ they become orthogonal, $|\phi_1\rangle = |+\rangle$, $|\psi_1\rangle = |-\rangle$. In both cases the randomness generation rate vanishes, as expected. However, we observe that for an infinitesimally small but nonvanishing angle, we achieve near-maximal randomness for $\eta = 1$, indicating that any amount of nonorthogonality in this scenario forces Eve to provide the honest measurement. More specifically, the $\eta = 1$ line coincides with the classical min-entropy from Eq. (23). However, the feature of much

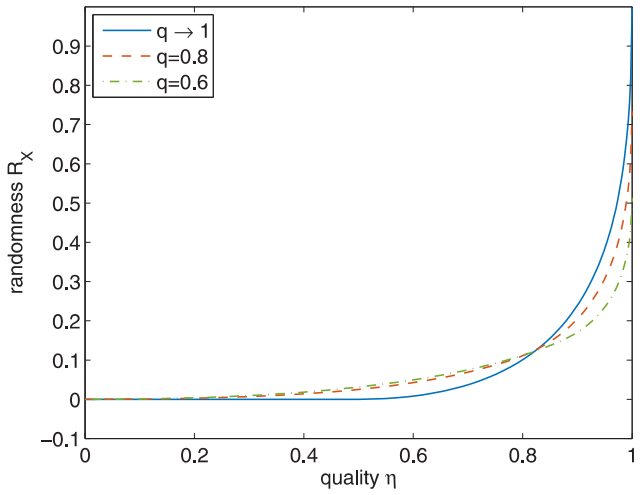

FIG. 5. The randomness rate of a two-state two-outcome setup with the sent states $|+\rangle$, $|0\rangle$ and different asymmetry parameters $q \equiv p_1$. The ideal measurement statistics corresponds to a σ_z measurement. The $q \to 1$ line is nonzero for $\eta > \frac{1}{2}$.

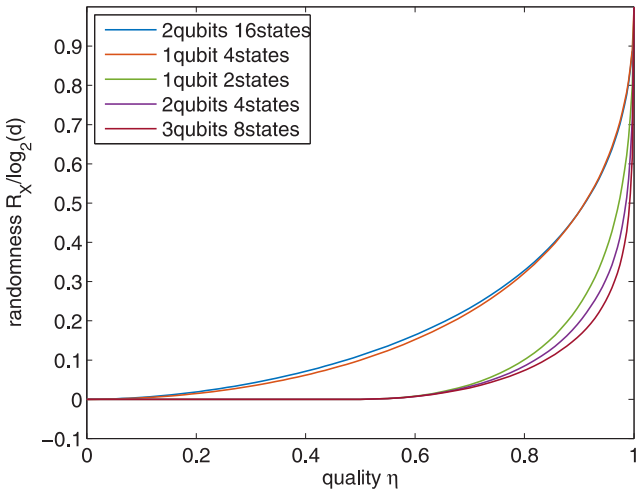

FIG. 6. The randomness rate per qubit versus the detector quality from Eq. (22) for different setups in the asymptotic limit (order from upper to lower line corresponds to order in legend). The upper two lines correspond to setups with four different sent states per qubit, whereas the lower three lines correspond to two different sent states per qubit. The ideal measurement statistics is given by a $\sigma_z^{\otimes m}$ measurement, where m is the number of sent qubits.

randomness for almost no quantumness comes at the cost of two requirements: (i) precisely characterized states to ensure that they are not identical and (ii) precise determination of the observed measurement statistics P_{obs}, because the randomness rate is discontinuous at $\alpha = 0$, where no randomness can be extracted. Thus, in practice one would use a preparation with a finite parameter α, such that the experimentally observed statistics allow to distinguish the two states.

2. The role of the asymmetry

In the asymptotic limit, and for a tomographically complete set of sent states, a higher asymmetry [i.e., higher probability to send $\rho(1)$] amounts to a larger gain in randomness for all detector qualities. However, we make the intriguing observation that for two sent qubit states $\{|+\rangle, |0\rangle\}$, the optimal asymmetry $q \equiv p_1$ depends on the detector quality. For that, we make use of an ideal statistics of a σ_z measurement. Figure 5 shows that for detector qualities $\eta \gtrsim 0.8$ maximal asymmetry $q \to 1$ is optimal, whereas for lower qualities a more balanced input distribution performs better. This behavior is possible in the two-state case, since there are uncharacterized detector degrees of freedom that can be optimized for Eve. In particular, there are two opposing effects. On the one hand, the maximally achievable randomness is upper bounded by the conditional min-entropy from Eq. (23), which is maximal in the asymmetric case, since for $q \to 1$ ($q = 0.6$) the upper bound is 1 ($\approx$0.51) at $\eta = 1$. However, with increasing unbiased noise (lower η), the difference between the upper bounds goes to zero. On the other hand, for low detector qualities, Eve can be perfectly correlated with the measurement outcomes of one state ($|+\rangle$) while reproducing P_{obs}. In this case, the measurement outcomes of the $|0\rangle$ state contain unpredictable randomness, provided η is nonzero. In such cases, the asymmetric rate $\mathcal{R}_X$ is equal to zero, but sending both states with similar probability leads to nonzero $\mathcal{R}_X$.

B. Multiple-qubit setups

1. Performance comparison

Here, we compare setups consisting of a sending device with states of dimension d and a measurement box with $n_o = d$ outcomes. In particular, the sent states are tensor products of m single-qubit states which are drawn from either the first two or all elements of the set $\{|+\rangle, |0\rangle, |1\rangle, |+i\rangle\}$. The measurement statistics is described by Eq. (22), where P_{id} is the distribution where the honest device implements a $\sigma_z^{\otimes m}$ measurement. We consider the asymmetric limit, in which the first state $|+\rangle^{\otimes m}$ is sent almost always. To account for experimental resources, we normalize the randomness gain to the state dimension: $\mathcal{R}_X / \log_2 d$, which is the randomness rate per qubit.

Figure 6 depicts the randomness rate per qubit for several numbers of sent qubits, $m = 1,2,3$, per round. States drawn from a tomographically complete set in test rounds are clearly advantageous, as the upper two lines show, since these allow for a better detector characterization. Within our noise model from Eq. (22), the normalized randomness gain is essentially independent of the number of sent qubits. More precisely, it slightly increases with dimension for four sent states per qubit (upper two lines), and slightly decreases with dimension for two sent states per qubit (lower three lines).

Furthermore, we have investigated entangled measurements, such as a Bell-state measurement, concluding that these do not generate more randomness and thus provide no advantage for increased experimental complexity.

2. Individual versus coherent attacks for two copies

Next, we wish to compare the performance of a single-qubit setup with a two-qubit setup, in which all observable quantities correspond to two independent copies of the single setup. This allows us to assess whether coherent attacks, which

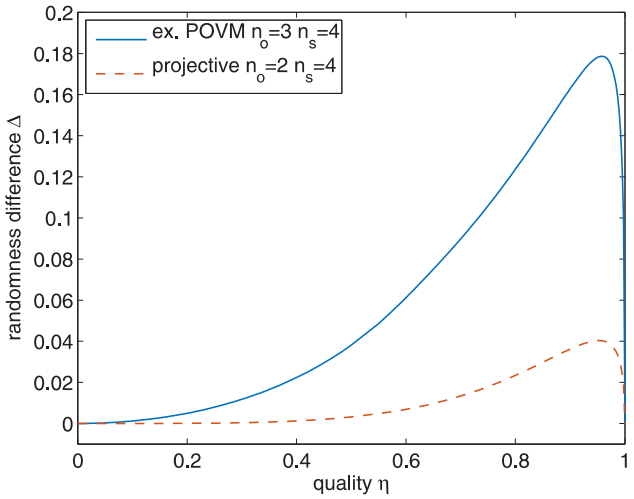

FIG. 7. The difference of the normalized randomness rates of a one-qubit setup with tomographically complete states, and a two-qubit doubling in the asymptotic limit. The solid line corresponds to a three-outcome POVM, whose statistics is determined by the measurement directions in Eq. (27), and the dashed line to a projective measurement.

act simultaneously on both qubits, provide an advantage over individual attacks. The results from Fig. 6 cannot be used for that, since there the two-qubit probability distribution is not the doubling of the one-qubit distribution.

Figure 7 shows the difference of normalized randomness generation $\Delta := \mathcal{R}_X(\text{1-qubit}) - \frac{1}{2}\mathcal{R}_X(\text{2-qubit})$ of a one-qubit setup with tomographically complete states, and a two-qubit doubling. The single-qubit statistics is given again by Eq. (22). The positive difference indicates that coherent attacks lead to more predictive power for Eve in the MDI setup. However, this assertion only holds if Eve can announce results of different round measurements simultaneously. It is an open question how Eve's predictive power behaves in a *sequential* setup, where she is forced to announce an outcome in each round, but the device can have a memory. This means that measurements of different rounds are in tensor product form and act in general on the postmeasurement state of all previous rounds, as well as a fresh ancilla [7].

V. CONCLUSION AND OUTLOOK

In this paper, we have introduced a general framework for randomness generation (i.e., expansion) with a well-characterized source of arbitrary quantum states and an untrusted detector with arbitrary measurements. We presented a randomness generation protocol and analyzed its achievable gain in randomness depending on the observed measurement statistics and sent states. A lower bound on the randomness rate is calculated by a numerically feasible semidefinite program.

As an application, we have discussed several examples of simple MDI setups and outlined optimal honest strategies. In particular, we devised a one-qubit MDI setup with four outcomes, which achieves more than one random bit per qubit for experimentally achievable detector efficiencies. These setups are practical compared to fully device-independent schemes, since no loophole-free Bell tests are required. Moreover, they achieve nonzero randomness generation even for low detector quality, whereas DI protocols abort in this scenario [5].

Generalizations of our result are possible by relaxing assumptions we have made. Of primary interest are attacks beyond the i.i.d. assumption. In this scenario, the i.i.d. assumption is relaxed to sequential (roundwise) interaction with the devices, including the possibility of a detector memory. For fully device-independent sequential randomness expansion, it has been shown [7] that for more than 10^8 rounds, the rate for general attacks is essentially the same as for i.i.d. attacks. We expect a similar behavior to hold in the case of MDI randomness expansion. The extension to a finite number of rounds is expected to be straightforwardly implementable in the SDP in Eq. (21). In analogy to parameter estimation in QKD, one can replace equality in the last constraint by an appropriate semidefinite constraint which includes the statistical deviation.

By comparison with previous work [16], we noticed that for the setup treated there, our lower bound to the randomness rate coincides with their exact rate. It is an open question whether this is the case in all MDI setups, which we leave for future work.

Note added. Recently, we became aware of related work [27], in which a comparable semidefinite program was used to calculate the MDI randomness rate in a two-qubit setup with tomographically complete states.

ACKNOWLEDGMENTS

The authors thank Matthias Kleinmann for discussion. F.B. acknowledges financial support from Evangelisches Studienwerk Villigst and from Strategischer Forschungsfonds (SFF) of the University of Düsseldorf. We acknowledge financial support from the German Federal Ministry of Education and Research (BMBF).

[1] D. Frauchiger, R. Renner, and M. Troyer, arXiv:1311.4547 (2013).
[2] R. Colbeck, Ph.D. thesis, University of Cambridge, 2009.
[3] Y. Z. Law *et al.*, J. Phys. A **47**, 424028 (2014).
[4] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).
[5] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, Nature (London) **464**, 1021 (2010).
[6] B. Christensen, K. McCusker, J. Altepeter, B. Calkins, T. Gerrits, A. Lita, A. Miller, L. Shalm, Y. Zhang, S. Nam *et al.*, Phys. Rev. Lett. **111**, 130406 (2013).
[7] R. Arnon-Friedman, R. Renner, and T. Vidick, arXiv:1607.01797 (2016).
[8] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán *et al.*, Nature (London) **526**, 682 (2015).

[9] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).
[10] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).
[11] A. Bednorz, Phys. Rev. A **95**, 042118 (2017).
[12] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).
[13] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Appl. **7**, 054018 (2017).
[14] T. Lunghi, J. B. Brask, C. Ci Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[15] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, New J. Phys. **17**, 113010 (2015).
[16] Z. Cao, H. Zhou, and X. Ma, New J. Phys. **17**, 125011 (2015).
[17] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Phys. Rev. A **94**, 060301(R) (2016).
[18] R. Renner, Int. J. Quantum Inf. **6**, 1 (2008).
[19] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[20] M. Tomamichel, arXiv:1203.2142 (2012).
[21] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).
[22] G. M. D'Ariano, P. L. Presti, and P. Perinotti, J. Phys. A **38**, 5979 (2005).
[23] E. Haapasalo, T. Heinosaari, and J.-P. Pellonpää, Quantum Inf. Proc. **11**, 1751 (2012).
[24] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Phys. Rev. A **93**, 040102(R) (2016).
[25] J. Lofberg, in *2004 IEEE International Symposium on Computer Aided Control Systems Design* (IEEE, New York, 2005), pp. 284–289.
[26] K.-C. Toh, M. J. Todd, and R. H. Tütüncü, Optim. Meth. Software **11**, 545 (1999).
[27] I. Šupić, P. Skrzypczyk, and D. Cavalcanti, Phys. Rev. A **95**, 042340 (2017).

A.2 Resource theory of coherence based on positive-operator-valued measures

Title:	Resource theory of coherence based on positive-operator-valued measures
Authors:	Felix Bischof, Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review Letters
Impact factor:	9.227 (2018)
Date of submission:	23 December 2018
Publication status:	Accepted
Contribution by F.B.:	First author (input approx. 85%)

This publication corresponds to the Bibliography entry [BKB18]. A summary of the results is given in Sec. 7.4. The main idea and research objectives were devised in collaboration with my co-authors. I derived the resource measure and investigated its properties. Moreover, I constructed the free operations and provided the SDP to characterize them. In addition, I developed the relations between Naimark extensions to prove the consistency of our theory. The example based on the qubit trine POVM was analyzed by me. I performed all numerical computations and created the figures and plots. Finally, I prepared the manuscript together with my co-authors and gave the bibliography concerning the state of the art.

Resource theory of coherence based on positive-operator-valued measures

Felix Bischof,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany
(Dated: August 16, 2019)

Quantum coherence is a fundamental feature of quantum mechanics and an underlying requirement for most quantum information tasks. In the resource theory of coherence, incoherent states are diagonal with respect to a fixed orthonormal basis, i.e., they can be seen as arising from a von Neumann measurement. Here, we introduce and study a generalization to a resource theory of coherence defined with respect to the most general quantum measurements, i.e., to arbitrary positive-operator-valued measures (POVMs). We establish POVM-based coherence measures and POVM-incoherent operations which coincide for the case of von Neumann measurements with their counterparts in standard coherence theory. We provide a semidefinite program that allows to characterize interconversion properties of resource states, and exemplify our framework by means of the qubit trine POVM, for which we also show analytical results.

Quantum resource theories (QRTs) [1–3] provide a structured framework in which quantum properties such as entanglement, coherence and purity are described in a quantitative way. Every QRT is based on the notions of free states (which do not contain the resource) and free operations (which cannot create the resource). Building on these basic constituents, QRTs allow to determine the resource content in quantum states, the optimal distillation of the resource, and the possibility of interconversion between resource states via free operations.

In recent years, the resource theory of quantum coherence has received much attention [4–7]. In the standard resource theory of coherence, the free states or incoherent states are states that are diagonal in a fixed orthonormal basis of a d-dimensional Hilbert space $\mathcal{H}$. Incoherent states ρ_{I} can thus also be seen as arising from a von Neumann measurement $\mathbf{P} = \{P_i\}$ in this basis, i.e., $\rho_{\mathrm{I}} = \sum_i^d P_i \sigma P_i$ for some state $\sigma \in \mathcal{S}$, where $\mathcal{S}$ denotes the set of quantum states on $\mathcal{H}$, and the measurement operators P_i are mutually orthogonal rank-one projectors that form a complete set, $\sum_i^d P_i = \mathbb{1}$. Coherent states are those which are not of the above form. This notion of coherence has been generalized in two directions. In [8–10], a resource theory of superposition was studied, where the requirement of orthogonality of the basis was lifted. In [11], Åberg proposed a framework that can be seen as the definition of coherence with respect to a general projective measurement, where the orthogonal measurement operators P_i may be of higher rank. In this generalized resource theory of coherence the free states are block-diagonal.

It is an important question whether the notion of coherence as an intrinsic quantum property of states can be further extended and formulated with respect to the most general quantum measurements, i.e., positive-operator-valued measures (POVMs). In this letter, we answer this question in the affirmative by introducing a resource theory of quantum state coherence based on arbitrary POVMs. More precisely, we establish a *family* of POVM-based resource theories of coherence, as each POVM leads to a different resource theory. In the special case of rank-1 orthogonal projective measurements, our theory coincides with standard coherence theory. Note that our approach is distinct from the mentioned previous generalizations [8–10] in terms of free states and operations. A motivation for our work is the fact that POVMs are generally advantageous compared to projective measurements, see [12] for a survey. In addition, we show in [13] that coherence of a state with respect to a POVM can be interpreted as the cryptographic randomness generated by measuring the POVM on the state. That is, the amount of POVM-coherence in a state is equal to the unpredictability of measurement outcomes relative to an eavesdropper with maximal information about the state, generalizing results from [14].

For a POVM-based coherence theory, the first challenge is to identify a meaningful notion of free, POVM-incoherent, states. This is achieved via the Naimark theorem [15, 16] which states that any POVM can be extended to a projective measurement in a larger space. Our concept of POVM-coherence of states in $\mathcal{S}$ is linked to a generalized resource theory of coherence from [11] in the extended (Naimark) space, for which we denote the set of states as $\mathcal{S}'$. POVM-coherence can be interpreted as the coherence resource that is required to implement the POVM on a given state via the canonical Naimark extension. The latter is realized by coupling the state to a probe, performing a global unitary and measuring the probe. This is relevant as POVMs are usually implemented in this way in experiments [17–19]. If one views the probe as a measurement apparatus, POVM-based coherence is the bipartite coherence generated in the global state by this process.

Conceptually, our work describes a novel way to construct resource theories. Quantum states and operations from the system space are embedded into a larger space which is equipped with a resource theory, providing a derivated resource theory on the original space. For this reason, our work does not follow the standard construction method for a resource theory: our starting point is the definition of a POVM-based coherence measure, from which we construct free states and operations. We then provide a semidefinite program that characterizes all POVM-incoherent operations, making them accessible for efficient numerical computation. Finally, we apply our framework to the example of the qubit trine POVM, for which we study the coherence measure and characterize all incoherent unitaries.

In the following, we present our main results and their interpretation. Technical details and proofs from every section of the main text are provided in the corresponding section of the Supplemental Material [20], which includes Refs. [21–33].

POVM and Naimark extension— A POVM on $\mathcal{H}$ with n outcomes is a set $\mathbf{E} = \{E_i\}_{i=1}^n$ of positive semidefinite operators $E_i \geq 0$, called effects, which satisfy $\sum_i^n E_i = \mathbb{1}$. The probability

to obtain the i-th outcome when measuring ρ is given by $p_i(\rho) = \mathrm{tr}[E_i\rho]$. We denote by $\{A_i\}$ a set of measurement operators of $\mathbf{E}$, i.e., $E_i = A_i^\dagger A_i$. Each measurement operator A_i is only fixed up to a unitary U_i, as the transformation $A_i \to U_i A_i$ leaves E_i invariant. The i-th post-measurement state for a given A_i is $\rho_i = \frac{1}{p_i} A_i \rho A_i^\dagger$.

Let us remind the reader that according to the Naimark theorem [15, 16], every POVM $\mathbf{E} = \{E_i\}_{i=1}^n$ on $\mathcal{H}$, if embedded in a larger Hilbert space, the Naimark space $\mathcal{H}'$ of dimension $d' \geq d$, can be extended to a projective measurement $\mathbf{P} = \{P_i\}_{i=1}^n$ on $\mathcal{H}'$. The most general way to embed the original Hilbert space $\mathcal{H}$ into $\mathcal{H}'$ is via a direct sum, requiring

$$\mathrm{tr}[E_i\rho] = \mathrm{tr}[P_i(\rho \oplus 0)] \tag{1}$$

to hold for all states ρ in $\mathcal{S}$, where $\oplus$ denotes the orthogonal direct sum, and 0 is the zero matrix of dimension $d' - d$. We call any projective measurement $\mathbf{P}$ which fulfills Eq. (1) a Naimark extension of $\mathbf{E}$.

The embedding into a larger-dimensional space can also be performed via the so-called *canonical* Naimark extension [34, 35]: one attaches an ancilla or probe, initially in a fixed state $|1\rangle\langle 1|$, via a tensor product. We denote the map that performs the embedding by $\mathcal{E}[\rho] = \rho \otimes |1\rangle\langle 1|$ and the space of embedded states by $\mathcal{S}_\mathcal{E} = \mathcal{E}[\mathcal{S}]$. A suitable global unitary V describes the interaction between system and probe such that the resulting state is $\rho' := V(\rho \otimes |1\rangle\langle 1|)V^\dagger$. A von Neumann measurement on the probe leads to the same probabilities p_i as the POVM if

$$\mathrm{tr}[E_i\rho] = \mathrm{tr}[(\mathbb{1} \otimes |i\rangle\langle i|)\rho'] = \mathrm{tr}[P_i(\rho \otimes |1\rangle\langle 1|)] \tag{2}$$

holds for all states ρ in $\mathcal{S}$. Here we have included the unitary V into the projective measurement, i.e., $P_i := V^\dagger(\mathbb{1} \otimes |i\rangle\langle i|)V$. Thus, P_i has rank d. This type of Naimark extension is not optimal in terms of smallest additionally required dimension [36], but its structure allows for a simpler derivation of general results, and directly describes the possibility to implement a POVM in an experiment. Both described types of Naimark extensions are not unique.

Resource theory of block coherence— Åberg [11] introduced general measures for the degree of superposition in a mixed quantum state with respect to orthogonal decompositions of the underlying Hilbert space, thus pioneering the resource theory of coherence. Here we translate his work into the present-day language of resource theories and refer to it as resource theory of block coherence.

The set $\mathcal{I}$ of block-incoherent (or free) states ρ_{BI} arises via a projective measurement $\mathbf{P} = \{P_i\}_{i=1}^n$ on the set of quantum states $\mathcal{S}$, namely [11]

$$\rho_{\mathrm{BI}} = \sum_i P_i \sigma P_i = \Delta[\sigma], \quad \sigma \in \mathcal{S}, \tag{3}$$

where the rank of the orthogonal projectors P_i is arbitrary, and we have defined the *block-dephasing map* Δ. In this framework, coherence is not "visible" within a subspace given by the range of P_i, but only across different subspaces. If all P_i have rank one, the standard resource theory of coherence is recovered. Note that here we have intentionally chosen the same symbol P_i as in Eq. (2), as we shortly identify the two.

We refer to the largest class of (free) operations that cannot create block coherence as (maximally) *block-incoherent* (MBI) operations. A channel Λ_{MBI} on $\mathcal{S}$ is element of this class iff it maps any block-incoherent state to a block-incoherent state, i.e.,

$$\Lambda_{\mathrm{MBI}}[\mathcal{I}] \subseteq \mathcal{I}, \tag{4}$$

or equivalently $\Lambda_{\mathrm{MBI}} \circ \Delta = \Delta \circ \Lambda_{\mathrm{MBI}} \circ \Delta$. In standard coherence theory this class is referred to as maximally-incoherent operations (MIO).

The amount of block coherence contained in a state ρ with respect to a projective measurement $\mathbf{P}$ can be quantified by suitable measures. We call a real-valued positive function $C(\rho, \mathbf{P}) \geq 0$ a block-coherence measure iff it fulfills

i. *Faithfulness:* $C(\rho, \mathbf{P}) = 0 \Leftrightarrow \rho \in \mathcal{I}$,

ii. *Monotonicity:* $C(\Lambda_{\mathrm{MBI}}[\rho], \mathbf{P}) \leq C(\rho, \mathbf{P})$ for all Λ_{MBI},

iii. *Convexity:* $C(\sum_i p_i\rho_i, \mathbf{P}) \leq \sum_i p_i C(\rho_i, \mathbf{P})$ for all $\{\rho_i\}$, $p_i \geq 0$, $\sum_i p_i = 1$.

Several block-coherence measures were introduced in [11], and a general class of measures can be derived from distances that are contractive under quantum operations [20]. An important example is the relative entropy of block coherence, defined as

$$C_{\mathrm{rel}}(\rho, \mathbf{P}) = \min_{\sigma \in \mathcal{I}} S(\rho \| \sigma) = S(\Delta[\rho]) - S(\rho), \tag{5}$$

where $S(\rho\|\sigma) = \mathrm{tr}[\rho \log \rho - \rho \log \sigma]$ denotes the quantum relative entropy and $S(\rho) = -S(\rho\|\mathbb{1})$ is the von Neumann entropy. In standard coherence theory, the relative entropy of coherence has several important operational meanings [5, 14, 37], e.g., it quantifies the distillable coherence and coherence cost under the class MIO [6].

POVM-based coherence measures— The main idea of our approach is to define the coherence of a state ρ with respect to the POVM $\mathbf{E}$ via its canonical Naimark extension. This concept is visualized in Fig. 1.

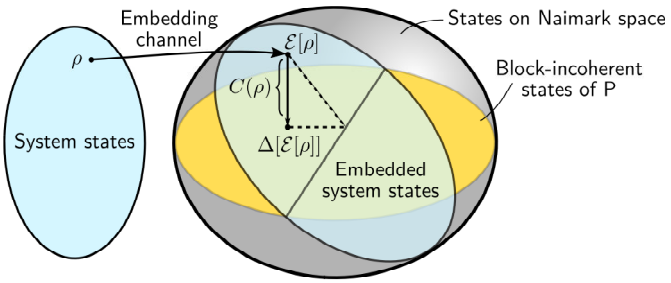

FIG. 1. We introduce a resource theory of POVM-based coherence by making use of the Naimark construction. Quantum states ρ are embedded as $\mathcal{E}[\rho] = \rho \otimes |1\rangle\langle 1|$ to act on a higher-dimensional Hilbert space (Naimark space). The POVM $\mathbf{E}$ is extended to a projective measurement $\mathbf{P}$ on the Naimark space, which defines a set of block-incoherent states $\mathcal{I}$. The POVM-coherence measure $C(\rho, \mathbf{E})$ is the distance between $\mathcal{E}[\rho]$ and its projection $\Delta[\mathcal{E}[\rho]]$ onto block-incoherent states.

Definition 1 (POVM-based coherence measure)**.** Let $C(\rho', \mathbf{P})$ be a unitarily-invariant block-coherence measure on $\mathcal{S}'$. The POVM-based coherence measure $C(\rho, \mathbf{E})$ for a state ρ in $\mathcal{S}$ is defined as the block coherence of the embedded state $\mathcal{E}[\rho] = \rho \otimes |1\rangle\langle 1|$ with respect to a canonical Naimark extension $\mathbf{P}$ of the POVM $\mathbf{E}$, namely

$$C(\rho, \mathbf{E}) \coloneqq C(\mathcal{E}[\rho], \mathbf{P}), \tag{6}$$

where the constraint in Eq. (2) has to hold. —It is straightforward to generalize this definition to the most general Naimark extension from Eq. (1).

The convexity of the underlying block-coherence measure directly implies that $C(\rho, \mathbf{E})$ is convex in ρ. Here, unitarily-invariant means that $C(\rho', \mathbf{P}) = C(U\rho' U^\dagger, U\mathbf{P}U^\dagger)$ holds for all unitaries U on $\mathcal{H}'$. This property ensures that $C(\rho, \mathbf{E})$ is invariant under a change of measurement operators $A_i \to U_i A_i$, with unitary U_i [20]. Note that the right side of Eq. (6) should also remain invariant if we employ a more general Naimark extension of $\mathbf{E}$ regarding dimension and form. We call measures with this property *well-defined*.

In this letter, we focus on the relative-entropy-based measure for which one can straightforwardly show that it is well-defined [20, 38]. See [13] for many further well-defined POVM-coherence measures.

Lemma 1 (Analytical form of a POVM-based coherence measure)**.** The relative entropy of POVM-based coherence $C_{\mathrm{rel}}(\rho, \mathbf{E})$ is convex and independent of the choice of Naimark extension for its definition. It admits the following form:

$$C_{\mathrm{rel}}(\rho, \mathbf{E}) = H(\{p_i(\rho)\}) + \sum_i p_i(\rho) S(\rho_i) - S(\rho), \tag{7}$$

with $p_i(\rho) = \mathrm{tr}[E_i \rho]$, $\rho_i = \frac{1}{p_i} A_i \rho A_i^\dagger$, and the Shannon entropy $H(\{p_i(\rho)\}) = -\sum_i p_i \log p_i$. In the special case of $\mathbf{E}$ being a von Neumann measurement, i.e., $E_i = |i\rangle\langle i|$, $C_{\mathrm{rel}}(\rho, \mathbf{E})$ equals the standard relative entropy of coherence.

The independence property holds because the eigenvalues of $\Delta[\mathcal{E}[\rho]]$ are the same for any two Naimark extensions used to define Δ and because the von Neumann entropy solely depends on the eigenvalues of its argument [20].

Minimal and maximal POVM-based coherence— We show in [20] that for an n-outcome POVM $\mathbf{E}$ the bounds $0 \leq C_{\mathrm{rel}}(\rho, \mathbf{E}) \leq \log n$ hold. However, there exist POVMs for which one or both of these bounds cannot be attained for any quantum state. First, let us discuss maximal coherence: the convexity of C_{rel} implies that its maxima are attained by the pure states that lead to the highest entropy of measurement outcomes, see [39] for a partial characterization.

Now, we address the lower bound. We can characterize POVM-incoherent states (i.e., states with zero POVM coherence) as follows.

Lemma 2 (Characterization of POVM-incoherent states)**.** Let $\mathbf{E} = \{E_i\}_{i=1}^n$ be a POVM and let $\bar{E}_i$ denote the projective part of E_i, i.e., the projector onto the eigenvalue-1 eigenspace of E_i. A state $\rho_{\mathrm{PI}} \in \mathcal{S}$ is POVM-incoherent with respect to $\mathbf{E}$ iff

$$\sum_i \bar{E}_i \rho_{\mathrm{PI}} \bar{E}_i = \rho_{\mathrm{PI}}. \tag{8}$$

By employing the canonical Naimark extension, one can show that ρ is POVM-incoherent iff $E_i \rho E_j = 0$ holds for all $i \neq j$, generalizing the requirement of vanishing off-diagonal elements for standard incoherent states. From this, Lemma 2 can be obtained [20], which implies that for particular POVMs the set of incoherent states $\mathcal{I}_{\mathrm{POVM}}$ is empty since no effect has a nonzero projective part. This includes any informationally complete POVM and the trine POVM which we discuss in detail below. The set $\mathcal{I}_{\mathrm{POVM}}$ may be empty because we decribe a derivated resource theory, i.e., a part of an encompassing framework in which free states exist. A resource theory where every object contains some resource is meaningful, since different objects can possess very different amounts of resource and are thus of different usefulness. In the following paragraph we introduce the set of POVM-incoherent operations which is nonempty, as it is defined via the Naimark extension. The generalization of $\mathcal{I}_{\mathrm{POVM}}$ is the set $\mathcal{M}$ of *minimally* POVM-coherent states that has similar properties as the standard incoherent set: it is nonemtpy, convex and closed under POVM-incoherent operations. Interestingly, the maximally mixed state $\rho = \frac{\mathbb{1}}{d}$ is not necessarily contained in $\mathcal{M}$ [13].

POVM-incoherent operations— The final main ingredient of our resource theory are quantum operations that cannot create POVM-based coherence, i.e., free operations. We denote maps acting on the larger space $\mathcal{S}'$ as Λ', while maps acting on the original system $\mathcal{S}$ are called Λ.

Definition 2 (POVM-incoherent operations)**.** Let $\mathbf{E}$ be a POVM and $\mathbf{P}$ any Naimark extension of it. Let Λ' be a completely positive trace-preserving map on $\mathcal{S}'$ that is

i. *Block-incoherent:* Λ' is block-incoherent (MBI) with respect to $\mathbf{P}$, see Eq. (4).

ii. *Subspace-preserving:* $\Lambda'[\mathcal{S}_\mathcal{E}] \subseteq \mathcal{S}_\mathcal{E}$ for the subset $\mathcal{S}_\mathcal{E} \subseteq \mathcal{S}'$ of embedded system states.

We call the channel $\Lambda_{\mathrm{MPI}} \coloneqq \mathcal{E}^{-1} \circ \Lambda' \circ \mathcal{E}$ on $\mathcal{S}$ a (maximally) POVM-incoherent (MPI) operation.

While this definition seems to be involved, it merely formalizes the feature that any MPI operation can be extended to an MBI map on a larger space. The second requirement in Def. 2 is necessary so that the POVM-incoherent channel only contains degrees of freedom of the original space $\mathcal{H}$.

Lemma 3 (Operations from Def. 2 cannot increase POVM-based coherence)**.** Let Λ_{MPI} be a POVM-incoherent operation of the POVM $\mathbf{E}$. Then, for any well-defined POVM-based coherence measure $C(\rho, \mathbf{E})$ it holds that

$$C(\Lambda_{\mathrm{MPI}}[\rho], \mathbf{E}) \leq C(\rho, \mathbf{E}). \tag{9}$$

For any measurement, we can characterize the set of POVM-incoherent operations by a semidefinite program (SDP), since

these operations are defined solely by linear conditions (i, ii and trace-preservation) and semidefinite conditions (complete positivity).

Theorem 1 (Characterization of POVM-incoherent operations)**.** The set MPI of POVM-incoherent operations is independent of the chosen Naimark extension and can be characterized by a semidefinite feasibility problem (SDP). In the special case of von Neumann measurements, MPI operations are equivalent to MIO maps of the standard coherence theory.

The independence property holds because for every two Naimark extensions of a POVM, any block-incoherent map on the larger Naimark space can be identified with a block-incoherent map on the smaller Naimark space which leads to the same (local) POVM-incoherent map [20].

Regarding the interconversion of resource states in our POVM-based coherence theory, we can employ the SDP characterization of POVM-incoherent operations Λ_{MPI} for a POVM $\mathbf{E}$ to determine numerically the maximally achievable fidelity $F_{\max}(\rho,\sigma) = \max_{\Lambda_{\mathrm{MPI}}} F(\Lambda_{\mathrm{MPI}}[\rho],\sigma)$ between a target state σ and $\Lambda_{\mathrm{MPI}}[\rho]$, see the Supplemental Material [20]. The fidelity $F(\rho,\sigma) = \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$ quantifies how close two quantum states ρ,σ are.

Example: qubit trine POVM— As an example, we analyze the case of the qubit trine POVM $\mathbf{E}^{\mathrm{trine}} = \{\frac{2}{3}|\phi_k\rangle\langle\phi_k|\}_{k=1}^{3}$, with measurement directions $|\phi_k\rangle = 1/\sqrt{2}(|0\rangle + \omega^{k-1}|1\rangle)$, where $\omega = \exp(2\pi i/3)$. The corresponding POVM-based coherence of *pure* states is illustrated in Fig. 2 (left). For the qubit trine POVM there are two states with maximal POVM-coherence $C_{\mathrm{rel}}^{\max} = \log 3$, namely $|\Psi_{\mathrm{m}}\rangle \in \{|0\rangle,|1\rangle\}$. The set $\mathcal{M}$ of states with minimal POVM-based coherence $C_{\mathrm{rel}}^{\min} = \log 3 - 1$ contains solely the maximally mixed state, $\mathcal{M} = \{\frac{\mathbb{1}}{2}\}$.

Regarding POVM-incoherent (free) operations, the free *unitary* operations can be fully characterized: up to a global phase there exist exactly six POVM-incoherent unitaries U_i^{trine}. They correspond to the rotations on the Bloch sphere that map the trine star to itself, i.e., the symmetry group of the equilateral triangle. In standard coherence theory the measurement map $\rho \to \Delta[\rho]$ is incoherent. However, for a general POVM the measurement map $\rho \to \sum_i \sqrt{E_i}\rho\sqrt{E_i}$ is not necessarily POVM-incoherent with respect to $\mathbf{E}$ as one can find POVMs for which the map increases the coherence of a state [13]. Notably, for the trine POVM $\mathbf{E}^{\mathrm{trine}}$, the SDP from Thm. 1 verifies that the measurement map is indeed POVM-incoherent. As to conversion properties, every qubit state ρ can be obtained deterministically by applying some POVM-incoherent operation to a maximally coherent state $|\Psi_{\mathrm{m}}\rangle \in \{|0\rangle,|1\rangle\}$. By applying the SDP, we have numerical evidence that given a state $|\psi\rangle \neq |\Psi_{\mathrm{m}}\rangle$, the only pure states that can be obtained from it with certainty via free operations are in the orbit $\{U_i^{\mathrm{trine}}|\psi\rangle\}$ under the trine-incoherent unitaries. An example for the conversion fidelity when starting from an initial state with less than maximal resource is shown in Fig. 2 (right).

Conclusion and Outlook— We have introduced a familiy of resource theories which quantify the coherence of a quantum state with respect to any given POVM. These resource theories are derived from the resource theory of block coherence [11]

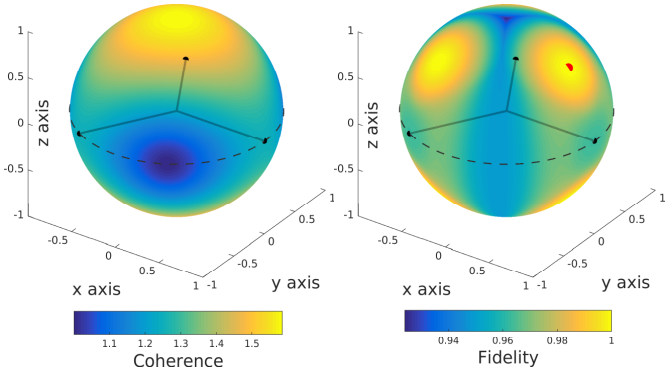

FIG. 2. POVM-based coherence theory for qubit states with respect to the trine POVM $\mathbf{E}^{\mathrm{trine}}$ in the Bloch sphere representation. Gray lines indicate the three measurement directions. *Left:* POVM-based coherence of pure qubits (surface of sphere). The states $|0\rangle$ and $|1\rangle$ have maximal coherence of $C = \log 3$. The Bloch vectors of the three states with the lowest pure-state coherence $C = 1$ are antipodal to the measurement directions. *Right:* Maximally achievable conversion fidelity $F_{\max}(\rho,\sigma) = \max_{\Lambda_{\mathrm{MPI}}} F(\Lambda_{\mathrm{MPI}}[\rho],\sigma)$ between a pure initial state ρ (red dot) subjected to POVM-incoherent operations Λ_{MPI} and a pure target state σ on the sphere surface. Here, $\rho = |\psi\rangle\langle\psi|$ with $|\psi\rangle = \cos(\frac{\pi}{8})|0\rangle + \sin(\frac{\pi}{8})|1\rangle$. Only states in the orbit of $|\psi\rangle$ under the six POVM-incoherent unitaries can be reached with unit fidelity, as depicted by the yellow spots.

via the Naimark extension on a higher-dimensional space. The restriction to the embedded original space led to the characterization of free states, free operations and resulting conversion properties within the POVM-based resource theories. For the case of von Neumann measurements, POVM-coherence measures and POVM-incoherent operations reduce to their counterparts in standard coherence theory.

Our approach has identified the coherence resource that is necessary to implement experimentally a general measurement on a given state via the Naimark extension. Also note other works that elucidate the role of quantum resources in the Naimark extension [40, 41].

Several open questions should be addressed in the future. First, it is not clear whether a characterization of POVM-incoherent operations without reference to the Naimark space is possible. A necessary condition is given by $\Lambda_{\mathrm{MPI}}[\mathcal{M}] \subseteq \mathcal{M}$, where $\mathcal{M}$ is the set of states with minimal POVM-based coherence. For projective measurements, this property is also sufficient as $\mathcal{M} = \mathcal{I}$. However, in general this property is not sufficient: for the trine POVM, $\mathcal{M} = \{\frac{\mathbb{1}}{2}\}$, thus the condition is equivalent to unitality, but there are unital maps that can increase the POVM-based coherence [20].

We expect that further consistent POVM-coherence measures can be introduced which have operational interpretations that generalize the results from standard coherence theory [42–47]. Finally, one can introduce the sub-class of *selective* POVM-incoherent operations, and study the corresponding conversion properties [13].

We acknowledge financial support from the German Federal Ministry of Education and Research (BMBF). F.B. gratefully acknowledges support from Evangelisches Studienwerk Villigst

and from Strategischer Forschungsfonds of the Heinrich Heine University Düsseldorf.

* felix.bischof@hhu.de

[1] F. G. S. L. Brandão and G. Gour, Physical Review Letters **115**, 070503 (2015).
[2] Z.-W. Liu, X. Hu, and S. Lloyd, Physical Review Letters **118**, 060502 (2017).
[3] E. Chitambar and G. Gour, Reviews of Modern Physics **91**, 025001 (2019).
[4] T. Baumgratz, M. Cramer, and M. B. Plenio, Physical Review Letters **113**, 140401 (2014).
[5] A. Winter and D. Yang, Physical Review Letters **116**, 120404 (2016).
[6] A. Streltsov, G. Adesso, and M. B. Plenio, Reviews of Modern Physics **89**, 041003 (2017).
[7] A. Streltsov, H. Kampermann, S. Wölk, M. Gessner, and D. Bruß, New Journal of Physics **20**, 053058 (2018).
[8] T. Theurer, N. Killoran, D. Egloff, and M. B. Plenio, Physical Review Letters **119**, 230401 (2017).
[9] K. C. Tan, T. Volkoff, H. Kwon, and H. Jeong, Physical Review Letters **119**, 190405 (2017).
[10] S. Das, C. Mukhopadhyay, S. S. Roy, S. Bhattacharya, A. Sen De, and U. Sen, arXiv:1705.04343 (2017).
[11] J. Åberg, arXiv:quant-ph/0612146 (2006).
[12] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Physical Review Letters **119**, 190501 (2017).
[13] F. Bischof, H. Kampermann, and D. Bruß, arXiv:1907.08574 (2019).
[14] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Physical Review A **92**, 022124 (2015).
[15] A. Peres, *Quantum Theory: Concepts and Methods*, vol. 57 (Springer Science & Business Media, 2006).
[16] T. Decker, D. Janzing, and M. Rötteler, Journal of Mathematical Physics **46**, 012104 (2005).
[17] G. N. M. Tabia, Physical Review A **86**, 062107 (2012).
[18] F. Becerra, J. Fan, and A. Migdall, Nature Communications **4**, 2028 (2013).
[19] M. Schiavon, G. Vallone, and P. Villoresi, Scientific Reports **6**, 30089 (2016).
[20] *See Supplemental Material at [URL will be inserted by publisher].*
[21] V. Vedral and M. B. Plenio, Physical Review A **57**, 1619 (1998).
[22] J. Matera, D. Egloff, N. Killoran, and M. B. Plenio, Quantum Science and Technology **1**, 01LT01 (2016).
[23] E. Chitambar, A. Streltsov, S. Rana, M. N. Bera, G. Adesso, and M. Lewenstein, Physical Review Letters **116**, 070402 (2016).
[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[25] J. C. A. Barata and M. S. Hussein, Brazilian Journal of Physics **42**, 146 (2012).
[26] F. Bischof, H. Kampermann, and D. Bruß, Physical Review A **95**, 062305 (2017).
[27] S. Boyd and L. Vandenberghe, *Convex optimization* (Cambridge University Press, 2004).
[28] N. J. Higham, C. Mehl, and F. Tisseur, SIAM Journal on Matrix Analysis and Applications **31**, 2163 (2010).
[29] T. F. Havel, Journal of Mathematical Physics **44**, 534 (2003).
[30] C. J. Wood, J. D. Biamonte, and D. G. Cory, Quantum Information & Computation **15**, 0579 (2015).
[31] M. Piani, Physical Review Letters **117**, 080401 (2016).
[32] J. Watrous, arXiv:1207.5726 (2012).
[33] Z. Bai and S. Du, Quantum Information & Computation **15**, 1355 (2015).
[34] M. M. Wilde, in *Proc. R. Soc. A* (The Royal Society, 2013), vol. 469.
[35] C. Sparaciari and M. G. A. Paris, Physical Review A **87**, 012106 (2013).
[36] P.-X. Chen, J. A. Bergou, S.-Y. Zhu, and G.-C. Guo, Physical Review A **76**, 060303(R) (2007).
[37] X. Yuan, Q. Zhao, D. Girolami, and X. Ma, arXiv:1605.07818 (2016).
[38] A. E. Rastegin, Journal of Physics A: Mathematical and Theoretical **51**, 414011 (2018).
[39] A. Szymusiak, arXiv:1701.01139 (2017).
[40] A. Streltsov, H. Kampermann, and D. Bruß, Physical Review Letters **106**, 160401 (2011).
[41] R. Jozsa, M. Koashi, N. Linden, S. Popescu, S. Presnell, D. Shepherd, and A. Winter, Quantum Information & Computation **3**, 405 (2003).
[42] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, Physical Review Letters **116**, 150502 (2016).
[43] T. Biswas, M. G. Díaz, and A. Winter, Proc. R. Soc. A **473**, 20170170 (2017).
[44] K. Bu, U. Singh, S.-M. Fei, A. K. Pati, and J. Wu, Physical Review Letters **119**, 150405 (2017).
[45] C. Xiong and J. Wu, Journal of Physics A: Mathematical and Theoretical **51**, 414005 (2018).
[46] K. Korzekwa, S. Czachórski, Z. Puchała, and K. Życzkowski, New Journal of Physics **20**, 043028 (2018).
[47] Y. Liu, Q. Zhao, and X. Yuan, Journal of Physics A: Mathematical and Theoretical **51**, 414018 (2018).

Supplemental Material

In the following we provide the technical details and proofs that complement the main text. In part A we give a detailed description of the Naimark extension of a POVM. Subsequently, in part B we describe the resource theory of block coherence [1] in a way that is analogous to standard coherence theory. The rest of the Supplemental Material is devoted to our resource theory of POVM-based coherence, which we formulate in the main text. In part C, we discuss general POVM-based coherence measures, including the relative entropy of POVM-based coherence on which we focus for the remainder of the paper. Achievable lower and upper bounds for the POVM-based coherence of quantum states are discussed in part D. In part E we prove properties of POVM-incoherent operations, i.e., free operations, and present explicitly the semidefinite program that characterizes them. Moreover, we study the conversion of resource states under free operations. Finally, in part F we exemplify all general results by means of the qubit trine POVM and provide analytical results of its POVM-based coherence theory.

Symbol	Explanation
$\mathcal{H}$	d-dimensional Hilbert space
$\mathcal{H}'$	d'-dimensional (Naimark) Hilbert space
$\mathcal{S}$	set of (system) quantum states on $\mathcal{H}$
$\mathcal{S}'$	set of quantum states on $\mathcal{H}'$
$\mathcal{E}$	embedding channel, from $\mathcal{S}$ to $\mathcal{S}'$
$\mathcal{H}_\mathcal{E}$	subspace of $\mathcal{H}'$ of embedded state vectors
$\Pi_\mathcal{E}$	orthogonal projector onto $\mathcal{H}_\mathcal{E}$
$\mathcal{S}_\mathcal{E}$	subset of $\mathcal{S}'$ of embedded system states
Ω	projector onto operators on $\mathcal{H}_\mathcal{E}$
$\mathbf{E}$	POVM on $\mathcal{H}$
$\{A_i\}$	set of measurement operators of $\mathbf{E}$
V	Naimark interaction unitary on $\mathcal{H}'$
$\mathbf{P}$	Naimark extension of $\mathbf{E}$ on $\mathcal{H}'$
Δ	Block-dephasing operation defined by $\mathbf{P}$
$\mathcal{I}$	set of block-incoherent states w.r.t. $\mathbf{P}$
$\mathcal{I}_\mathrm{POVM}$	set of POVM-incoherent states w.r.t. $\mathbf{E}$
ρ_PI	POVM-incoherent state w.r.t. $\mathbf{E}$
Λ'_MBI	block-incoherent operation on $\mathcal{S}'$
$\Lambda'\vert_{\mathcal{S}_\mathcal{E}}$	embedded POVM-incoherent operation
Λ_MPI	POVM-incoherent operation on $\mathcal{S}$

TABLE I. Notation used throughout this work.

Appendix A: POVM and Naimark extension

In this part, we provide the details and construction of the Naimark extension of a POVM $\mathbf{E}$. Under a general Naimark extension we understand any projective measurement $\mathbf{P} = \{P_i\}$ on $\mathcal{H}'$, which fulfills Eq. (1). Consequently, the uppper left $d \times d$ block of the Naimark extension effect P_i coincides with the POVM effect E_i, i.e., for $\Pi_\mathcal{E} = \mathbb{1}_d \oplus 0_{d'-d}$ it holds that

$$E_i \oplus 0_{d'-d} = \Pi_\mathcal{E} P_i \Pi_\mathcal{E}. \tag{A1}$$

Therefore, it is convenient to embed system operators X on $\mathcal{H}$ into the Naimark space $\mathcal{H}'$ via the *isometric* embedding map $\mathcal{E}[X] \coloneqq X \oplus 0$ and call $\mathcal{H}_\mathcal{E} \coloneqq \{|\psi\rangle \oplus 0 : |\psi\rangle \in \mathcal{H}\}$ the embedded state space. Now, we only need to consider (embedded) operators on the Naimark space $\mathcal{H}'$. The construction of a projective measurement fulfilling Eq. (A1) is straigthforward. We provide details for the *canonical* Naimark extension, for which the Naimark space has product form $\mathcal{H}' = \mathcal{H} \otimes \mathcal{H}_R$, with $\mathcal{H}_R$ being the probe's state space. In this case, we employ the embedding map $\mathcal{E}[X] \coloneqq X \otimes |1\rangle\langle 1|$ and $\mathcal{H}_\mathcal{E} = \mathcal{H} \otimes |1\rangle$. The canonical Naimark extension is generally not of the smallest possible dimension $d'_\mathrm{min} = \sum_i \operatorname{rank} E_i$ [2]. In section C (E) we show that POVM-based coherence measures (POVM-incoherent operations) are independent of the choice of Naimark extension.

Let $\mathbf{E} = \{E_i\}_{i=1}^n$ be an n-outcome POVM on $\mathcal{H}$, and $\{A_i\}$ a set of measurement operators for $\mathbf{E}$. Any measurement operator can be written as $A_i = U_i \sqrt{E_i}$ for some unitary operator U_i. Let $\{|i\rangle\}$ be an orthonormal basis of the probe space $\mathcal{H}_R$ and define the operator

$$\tilde{V} = \sum_{i=1}^n A_i \otimes |i\rangle\langle 0|, \tag{A2}$$

which is an isometry from $\mathcal{H}_\mathcal{E}$ to $\mathcal{H}'$, i.e., it fulfills $\tilde{V}^\dagger \tilde{V} = \mathbb{1}_d$ on $\mathcal{H}_\mathcal{E}$ as a consequence of the normalization of the POVM. The isometry $\tilde{V}$ can be extended to a unitary V on $\mathcal{H}'$ by completing the set of orthonormal column vectors (lying in $\operatorname{im} \tilde{V} \subseteq \mathcal{H}'$) to an orthonormal basis, i.e., by filling up the columns of the $nd \times d$ matrix to an $nd \times nd$ matrix with orthonormal column vectors. Now, we can parameterize the unitary by operators $A_{i,a}$ on $\mathcal{H}$ as

$$V = \sum_{i,a=1}^n A_{i,a} \otimes |i\rangle\langle a|, \tag{A3}$$

where $A_{i,1} = A_i$. To ensure the unitary condition $V^\dagger V = V V^\dagger = \mathbb{1}_{d'}$, these operators need to fulfill

$$\sum_i A_{i,a}^\dagger A_{i,b} = \delta_{a,b} \mathbb{1}_d, \quad \text{and}$$
$$\sum_a A_{i,a} A_{j,a}^\dagger = \delta_{i,j} \mathbb{1}_d. \tag{A4}$$

Finally, the canonical Naimark extension $\mathbf{P} = \{P_i\}_{i=1}^n$ of $\mathbf{E}$ is defined as

$$\begin{aligned} P_i &\coloneqq V^\dagger \mathbb{1} \otimes |i\rangle\langle i| V \\ &= \sum_{a,b} A_{i,a}^\dagger A_{i,b} \otimes |a\rangle\langle b|, \end{aligned} \tag{A5}$$

which is a rank-d projective measurement, i.e., $\operatorname{rank} P_i = d$ and $P_i P_j = \delta_{i,j} P_j$. Projecting this measurement onto the embedded state space $\mathcal{H}_\mathcal{E}$ with the projector $\Pi_\mathcal{E} = \mathbb{1} \otimes |1\rangle\langle 1|$ yields the embedding of the POVM $\mathbf{E}$,

$$\Pi_\mathcal{E} P_i \Pi_\mathcal{E} = A_{i,1}^\dagger A_{i,1} \otimes |1\rangle\langle 1| = E_i \otimes |1\rangle\langle 1| = \mathcal{E}[E_i]. \tag{A6}$$

This property implies that

$$\operatorname{tr}[E_i \rho] = \operatorname{tr}[P_i (\rho \otimes |1\rangle\langle 1|)], \tag{A7}$$

and thus, up to an exchange of the two subsystems the Naimark extension property from Eq. (1).

Appendix B: Resource theory of block coherence

In this part, we supplement details of the resource theory of block coherence as described in the main text. This theory was introduced in [1] and we formulate it in a modern way that is analogous to the resource theory of coherence [3].

Let $\mathbf{P} = \{P_i\}_{i=1}^n$ be a projective measurement on $\mathcal{H}$. Resource-free states, called block-incoherent, are block-diagonal with respect to $\mathbf{P}$ and belong to the set

$$\mathcal{I} = \{\rho_{\mathrm{BI}} = \sum_i P_i \sigma P_i : \sigma \in \mathcal{S}\}. \tag{B1}$$

Therefore, block-incoherent states are characterized as the image of the block-dephasing operator $\Delta[\sigma] = \sum_i P_i \sigma P_i$ applied to any state σ. By the mutual orthogonality of the effects P_i, block-incoherent states are also characterized by the condition

$$\rho \in \mathcal{I} \Leftrightarrow P_i \rho P_j = 0 \quad \forall i \neq j \in \{1, \ldots, n\}. \tag{B2}$$

Let $C(\rho, \mathbf{P})$ be a block-coherence measure as defined in the main text. Any block-coherence measures obeys a further desirable property, which ensures that it does not depend on the choice of basis within the blocks (subspaces) $\pi_i := \mathrm{im}\, P_i$.

Proposition 1. Every block-coherence measure $C(\rho, \mathbf{P})$ as defined in the main text also fulfills

iii. *Block-unitary invariance:* $C(U\rho U^\dagger, \mathbf{P}) = C(\rho, \mathbf{P})$ with $U = \oplus_i U_i$, and where U_i is unitary on π_i.

Proof. The assertion holds since U is a reversible block-incoherent operation and thus the monotonicity property holds with equality. More precisely, it holds that $P_i U = U P_i$ and therefore $U\Delta[\sigma]U^\dagger = \Delta[U\sigma U^\dagger]$. Because block-incoherent states have the form $\rho = \Delta[\sigma]$, we conclude that $U\rho U^\dagger \in \mathcal{I}$ for all states $\rho \in \mathcal{I}$. Hence, the unitary channel $\rho \to U\rho U^\dagger$ is a maximally-block-incoherent (MBI) operation. Since unitary channels are invertible, we can apply the monotonicity property in both directions to obtain equality, from which the assertion follows. □

Several block-coherence quantifier were introduced in [1], and the monotonicity condition was proven for some of them. We consider a general class of a block-coherence quantifier that is obtained from a distance $D(\rho, \sigma)$ via

$$C(\rho, \mathbf{P}) := \inf_{\sigma \in \mathcal{I}} D(\rho, \sigma). \tag{B3}$$

Certain properties of the distance measure lead to the block-coherence measure properties.

Proposition 2. The distance-based block-coherence quantifier $C(\rho, \mathbf{P}) = \inf_{\sigma \in \mathcal{I}} D(\rho, \sigma)$ fulfills

i. *Positivity and Faithfulness*, if the distance $D(\rho, \sigma)$ is non-negative and vanishes if and only if $\rho = \sigma$.

ii. *Monotonicity*, if the distance is contractive under quantum operations Λ, that is, $D(\Lambda[\rho], \Lambda[\sigma]) \leq D(\rho, \sigma)$.

Proof. The proof of the second assertion is analogous to the case of coherence theory [3, 4]. For convenience, we outline it here,

$$\begin{aligned} C(\rho, \mathbf{P}) &= \inf_{\sigma \in \mathcal{I}} D(\rho, \sigma) = D(\rho, \sigma^*) \\ &\geq D(\Lambda_{\mathrm{MBI}}[\rho], \Lambda_{\mathrm{MBI}}[\sigma^*]) \\ &\geq \inf_{\tau \in \mathcal{I}} D(\Lambda_{\mathrm{MBI}}[\rho], \tau) \\ &= C(\Lambda_{\mathrm{MBI}}[\rho]), \end{aligned} \tag{B4}$$

where σ^* denotes a state that achieves the minimum. The first inequality follows from the contractive property of the distance, and the second equality holds because $\Lambda_{\mathrm{MBI}}[\sigma^*] \in \mathcal{I}$. □

In the following, we focus on the relative-entropy-based block-coherence measure which was introduced in [1]. The relative entropy of block coherence is defined as

$$C_{\mathrm{rel}}(\rho) := \min_{\sigma \in \mathcal{I}} S(\rho \| \sigma), \tag{B5}$$

where $S(\rho \| \sigma)$ denotes the quantum relative entropy. The coherence quantifier $C_{\mathrm{rel}}(\rho)$ is convex and satisfies nonnegativity. Moreover, the monotonicity property is proven in the following Proposition.

Proposition 3. The relative entropy of block coherence is a block-coherence measure and admits the following simple form

$$C_{\mathrm{rel}}(\rho) = S(\Delta[\rho]) - S(\rho). \tag{B6}$$

Proof. The relative entropy is contractive under quantum operations [5] and thus $C_{\mathrm{rel}}(\rho)$ satisfies the monotonicity condition because of Prop. 2. The simplified form $C_{\mathrm{rel}}(\rho) = S(\Delta[\rho]) - S(\rho)$ was first stated in [1], and is proven analogous to coherence theory [6, 7]. For the convenience of the reader, we outline the proof. Observe that

$$\begin{aligned} \mathrm{tr}[\Delta[\rho] \log \sigma_{\mathrm{BI}}] &= \mathrm{tr}[\rho \Delta[\log \sigma_{\mathrm{BI}}]] \\ &= \mathrm{tr}[\rho \log \sigma_{\mathrm{BI}}], \end{aligned} \tag{B7}$$

for any block-incoherent state σ_{BI}, since the operator logarithm of a nonnegative matrix preserves the block-diagonal structure, as it only acts on the eigenvalues. This implies that

$$\begin{aligned} S(\rho \| \sigma_{\mathrm{BI}}) &= \mathrm{tr}[\rho \log \rho] - \mathrm{tr}[\rho \log \sigma_{\mathrm{BI}}] \\ &= -\mathrm{tr}[\Delta[\rho] \log \Delta[\rho]] + \mathrm{tr}[\rho \log \rho] \\ &\quad + \mathrm{tr}[\Delta[\rho] \log \Delta[\rho]] - \mathrm{tr}[\Delta[\rho] \log \sigma_{\mathrm{BI}}] \\ &= S(\Delta[\rho]) - S(\rho) + S(\Delta[\rho] \| \sigma_{\mathrm{BI}}). \end{aligned} \tag{B8}$$

The third term is nonnegative, $S(\Delta[\rho] \| \sigma_{\mathrm{BI}}) \geq 0$, and therefore the minimum over block-incoherent states is achieved when it vanishes, i.e., $\sigma_{\mathrm{BI}} = \Delta[\rho]$. □

Appendix C: POVM-based coherence measures

In this part, we provide details and proofs concerning POVM-based coherence measures that are introduced in the main text as the first constituent of our resource theory.

First, we show that any POVM-based coherence measure inherits convexity from the underlying block-coherence measure.

Let $\{\rho_i\}$ be a set of quantum states from $\mathcal{S}$ and let $\{p_i\}$ be a probability distribution, i.e., $p_i \geq 0$, $\sum_i p_i = 1$. Then it holds that

$$C(\sum_i p_i\rho_i, \mathbf{E}) = C(\mathcal{E}[\sum_i p_i\rho_i], \mathbf{P}) = C(\sum_i p_i\mathcal{E}[\rho_i], \mathbf{P}) \leq \sum_i p_i C(\mathcal{E}[\rho_i], \mathbf{P}) = \sum_i p_i C(\rho_i, \mathbf{E}), \quad \text{(C1)}$$

where we have employed the linearity of the embedding channel $\mathcal{E}$ and the convexity of the block-coherence measure $C(\rho', \mathbf{P})$.

In the next proposition we focus on POVM-coherence measures derived from the canonical Naimark extension defined on $\mathcal{H} \otimes \mathcal{H}_R$.

Proposition 4. Let $C(\rho, \mathbf{E}) = C(\mathcal{E}[\rho], \mathbf{P})$ be a POVM-based coherence measure, evaluated on the canonical Naimark extension $\mathbf{P}$ of $\mathbf{E}$. The measure can also be expressed as

$$C(\rho, \mathbf{E}) = C(\mathcal{E}_V[\rho], \{\mathbb{1} \otimes |i\rangle\langle i|\}), \quad \text{(C2)}$$

where now the interaction V is attributed to the embedding $\mathcal{E}_V[\rho] = V\rho \otimes |1\rangle\langle 1|V^\dagger = \sum_{i,j} A_i \rho A_j^\dagger \otimes |i\rangle\langle j|$. The measure is invariant under a change of measurement operators, i.e., under the transformation $A_i \to U_i A_i$ with unitary U_i.

Proof. By definition of $C(\rho, \mathbf{E})$, $C(\rho', \mathbf{P})$ is a unitarily-invariant block-coherence measure, that is, $C(\rho', \mathbf{P}) = C(U\rho' U^\dagger, U\mathbf{P}U^\dagger)$ holds for all unitaries U on $\mathcal{H}'$ and all states $\rho' \in \mathcal{S}'$. Therefore, it holds that

$$\begin{aligned} C(\rho, \mathbf{E}) &= C(\mathcal{E}[\rho], \mathbf{P}) \\ &= C(\rho \otimes |1\rangle\langle 1|, \{V^\dagger \mathbb{1} \otimes |i\rangle\langle i| V\}) \\ &= C(V\rho \otimes |1\rangle\langle 1|V^\dagger, \{\mathbb{1} \otimes |i\rangle\langle i|\}) \\ &= C(\mathcal{E}_V[\rho], \{\mathbb{1} \otimes |i\rangle\langle i|\}), \end{aligned} \quad \text{(C3)}$$

where the third equality follows from unitary invariance.

This implies that $C(\rho, \mathbf{E})$ is invariant under a change of measurement operators, $A_i \to U_i A_i$, with unitary U_i, and is therefore well-defined. Indeed, the unitary transformation acts on the embedded state as $\mathcal{E}_V[\rho] \to \sum_{i,j} U_i A_i \rho A_j^\dagger U_j^\dagger \otimes |i\rangle\langle j| = U\mathcal{E}_V[\rho]U^\dagger$, with a block-diagonal unitary $U = \sum_i U_i \otimes |i\rangle\langle i|$. Since every block-coherence measure is invariant under block-diagonal unitaries, as shown in Prop. 1, the measure is invariant under a change of measurement operators. □

In the remainder of this part we prove Lemma 1 from the main text. For the claim that $C_{\text{rel}}(\rho, \mathbf{E})$ is independent of the chosen Naimark extension of a POVM $\mathbf{E} = \{E_i\}$, we consider any Naimark extension $\mathbf{P}$ of $\mathbf{E}$ as defined in Eq. (1), not necessarily of tensor product form. To do so, we employ the generalized definitions introduced in App. A,

$$\mathcal{E}[X] = X \oplus 0, \quad \mathcal{H}_\mathcal{E} = \{|\psi\rangle \oplus 0\}, \quad \Pi_\mathcal{E} = \mathbb{1} \oplus 0. \quad \text{(C4)}$$

Moreover, we define the generalized POVM-based coherence measure $C_{\text{rel}}(\rho, \mathbf{E})$ as

$$C_{\text{rel}}(\rho, \mathbf{E}) := S(\Delta[\rho \oplus 0]) - S(\rho). \quad \text{(C5)}$$

• *Proof of* **Lemma 1** *from main text.* First, we show that the POVM-based coherence measure obtained from the relative entropy $C_{\text{rel}}(\rho, \mathbf{E}) = C_{\text{rel}}(\rho \oplus 0, \mathbf{P})$ is independent of the choice of Naimark extension $\mathbf{P}$. We do that by showing that the eigenvalues of $\Delta[\rho \oplus 0]$ are the same for any two Naimark extensions used to define the dephasing Δ. The assertion then readily follows because the von Neumann entropy is a function of the eigenvalues of a state.

Let $\mathbf{P}$ on $\mathcal{H}'$ and $\hat{\mathbf{P}}$ on $\hat{\mathcal{H}}'$ be two Naimark extensions of the same POVM $\mathbf{E}$, such that without loss of generality $d' \geq \hat{d}'$ holds. We embed the smaller Hilbert space $\hat{\mathcal{H}}'$ canonically into the larger Hilbert space $\mathcal{H}'$ such that all operators on the smaller space are filled up appropriately with zeros. First, we show that $P_i\rho \oplus 0 P_i$ and $\hat{P}_i\rho \oplus 0\hat{P}_i$ have the same eigenvalues. By definition of the Naimark extension it holds that

$$\text{tr}[P_i\rho \oplus 0] = \text{tr}[\hat{P}_i\rho \oplus 0] \quad \text{(C6)}$$

for all system states $\rho \in \mathcal{S}$. If ρ is a pure state, $P_i\rho \oplus 0P_i$ and $\hat{P}_i\rho \oplus 0\hat{P}_i$ are both rank-1 operators that because of Eq. (C6) have the same nonzero eigenvalue. For the mixed state case, we consider the following. From the definition of the Naimark extension it follows that

$$\Pi_\mathcal{E} P_i P_i \Pi_\mathcal{E} = E_i \oplus 0 = \Pi_\mathcal{E} \hat{P}_i \hat{P}_i \Pi_\mathcal{E}, \quad \text{(C7)}$$

where $\hat{P}_i$ is extended to $\mathcal{H}'$, implying that $\sum_i \hat{P}_i$ is the projector onto $\hat{\mathcal{H}}'$. The equation follows from Eq. (C6) because the system states provide a POVM-tomography on the subspace $\mathcal{H}_\mathcal{E}$. It is known, that Eq. (C7) implies that there exists a unitary Q_i on $\mathcal{H}'$ such that

$$P_i\Pi_\mathcal{E} = Q_i\hat{P}_i\Pi_\mathcal{E}. \quad \text{(C8)}$$

Concretely, these matrices have singular value decomposition

$$P_i\Pi_\mathcal{E} = U_i \begin{pmatrix} \Sigma_{r_i} & \\ & 0 \end{pmatrix} V_i^\dagger, \quad \hat{P}_i\Pi_\mathcal{E} = \hat{U}_i \begin{pmatrix} \Sigma_{r_i} & \\ & 0 \end{pmatrix} V_i^\dagger, \quad \text{(C9)}$$

for some unitaries $U_i, \hat{U}_i, V_i$, $r_i = \text{rank}\, E_i$, and a $r_i \times r_i$ diagonal matrix Σ_{r_i} containing the square root of the nonzero eigenvalues of E_i. Then, the unitary is given by $Q_i = U_i\hat{U}_i^\dagger$. Now, the unitaries Q_i can be combined into a single unitary, by noting that the restriction $Q_i|_{\hat{\pi}_i}$ with $\hat{\pi}_i = \text{im}\,\hat{P}_i$ is a map from and to orthogonal subspaces $Q_i|_{\hat{\pi}_i} : \hat{\pi}_i \to \pi_i$. Thus, we can define the block-diagonal unitary $Q = \oplus_i Q_i|_{\hat{\pi}_i} \oplus \mathbb{1}$, where the last term is the identity on the subspace $(\hat{\mathcal{H}}')^\perp$ of $\mathcal{H}'$. With that, we have constructed a unitary Q that relates the two Naimark extension acting on the subspace $\mathcal{H}_\mathcal{E}$, namely $P_i\Pi_\mathcal{E} = Q\hat{P}_i\Pi_\mathcal{E}$. Consequently, $\Delta[\rho \oplus 0] = \sum_i P_i\Pi_\mathcal{E}(\rho \oplus 0)\Pi_\mathcal{E}P_i = Q\sum_i \hat{P}_i\Pi_\mathcal{E}(\rho \oplus 0)\Pi_\mathcal{E}\hat{P}_iQ^\dagger = Q\hat{\Delta}[\rho \oplus 0]Q^\dagger$ holds , i.e., $\Delta[\rho \oplus 0]$ and $\hat{\Delta}[\rho \oplus 0]$ have the same eigenvalues. Since the von Neumann entropy solely depends on the eigenvalues of its argument, we conclude that

$$\begin{aligned} C_{\text{rel}}(\rho \oplus 0, \mathbf{P}) &= S(\Delta[\rho \oplus 0]) - S(\rho) \\ &= S(\hat{\Delta}[\rho \oplus 0]) - S(\rho) \\ &= C_{\text{rel}}(\rho \oplus 0, \hat{\mathbf{P}}), \end{aligned} \quad \text{(C10)}$$

which means that $C_{\text{rel}}(\rho, \mathbf{E})$ is independent of the Naimark extension used to define it.

The relative entropy of POVM-based coherence admits an expression just in term of system degrees of freedom, i.e., without making reference to the Naimark space. We need to show that C_{rel}

can be expressed as $C_{\text{rel}}(\rho,\mathbf{E}) = H(\{p_i(\rho)\}) + \sum_i p_i(\rho)S(\rho_i) - S(\rho)$, with $p_i(\rho) = \text{tr}[E_i\rho]$, and $\rho_i = \frac{1}{p_i}A_i\rho A_i^\dagger$, and where S denotes the von-Neumann entropy, and H the Shannon entropy. Let $\Delta[\cdot] = \sum_i P_i \cdot P_i$ be the block-dephasing operator of the canonical Naimark extension $\mathbf{P} = \{V^\dagger \mathbb{1} \otimes |i\rangle\langle i|V\}$ with $V(\rho \otimes |1\rangle\langle 1|)V^\dagger = \sum_{i,j} A_i\rho A_j^\dagger \otimes |i\rangle\langle j|$. Then it holds that

$$\begin{aligned} C_{\text{rel}}(\rho,\mathbf{E}) &= C_{\text{rel}}(\rho\otimes|1\rangle\langle 1|,\mathbf{P}) \\ &= S(\Delta[\rho\otimes|1\rangle\langle 1|]) - S(\rho\otimes|1\rangle\langle 1|) \\ &= S(\sum_i \mathbb{1}\otimes|i\rangle\langle i|V(\rho\otimes|1\rangle\langle 1|)V^\dagger\mathbb{1}\otimes|i\rangle\langle i|) - S(\rho) \\ &= S(\sum_i A_i\rho A_i^\dagger\otimes|i\rangle\langle i|) - S(\rho) \\ &= S(\sum_i p_i\rho_i\otimes|i\rangle\langle i|) - S(\rho) \\ &= H(\{p_i(\rho)\}) + \sum_i p_i S(\rho_i) - S(\rho), \end{aligned} \tag{C11}$$

where the last equality follows from the joint entropy theorem [8]. □

Appendix D: Minimal and maximal POVM-based coherence

In this part, we prove the characterization of POVM-incoherent states from Lemma 2. Moreover, we show general upper and lower bounds on $C_{\text{rel}}(\rho,\mathbf{E})$ and discuss classes of POVMs for which these bounds can or cannot be attained.

Proposition 5. A state ρ is POVM-incoherent with respect to a POVM $\mathbf{E} = \{E_i\}_{i=1}^n$ iff the following holds:

$$E_i\rho E_j = 0 \quad \forall\ i \neq j \in \{1,\dots,n\}\ . \tag{D1}$$

Proof. We need to show that $C_{\text{rel}}(\rho,\mathbf{E}) = C_{\text{rel}}(\rho\otimes|1\rangle\langle 1|,\mathbf{P}) = 0$ is equivalent to $E_i\rho E_j = 0\ \forall\ i \neq j \in \{1,\dots,n\}$. The set $\mathcal{I}$ of block-incoherent states with respect to the canonical Naimark extension $\mathbf{P} = \{V^\dagger\mathbb{1}\otimes|i\rangle\langle i|V\}$ is composed of states of the form

$$\mathcal{I} = \{V^\dagger \sum_i p_i\rho_i\otimes|i\rangle\langle i|V\}, \tag{D2}$$

as these are the states that are invariant under the dephasing operation $\Delta[\cdot] = \sum_i P_i\cdot P_i$. Here, $\{\rho_i\}$ is a set of states and $\{p_i\}$ a probability distribution. A state $\rho\otimes|1\rangle\langle 1| \in \mathcal{S}_\mathcal{E}$ is of the above form if and only if $V\rho\otimes|1\rangle\langle 1|V^\dagger = \sum_i p_i\rho_i\otimes|i\rangle\langle i|$, which is equivalent to

$$\begin{aligned} &\sum_{i,j} A_i\rho A_j^\dagger\otimes|i\rangle\langle j| = \sum_i p_i\rho_i\otimes|i\rangle\langle i| \\ \Leftrightarrow\ & A_i\rho A_j^\dagger = 0\ \ \forall\ i\neq j\in\{1,\dots,n\}. \end{aligned} \tag{D3}$$

Since $E_i = A_i^\dagger A_i$, the condition (D3) implies $E_i\rho E_j = 0\ \forall\ i \neq j \in \{1,\dots,n\}$. The converse implication is also true which can be seen by employing the Moore-Penrose inverse X^- of a matrix X [9]. It has the properties $X^-X = \Pi_{\text{supp}\,X}$, and $XX^- = \Pi_{\text{im}\,X}$, with the projectors onto the support and image of X, respectively. Together with $\text{supp}\,X^\dagger = \text{im}\,X$ and $\text{supp}\,X^\dagger = \text{im}\,X$ it follows that

$$\begin{aligned} & E_i\rho E_j = 0 \\ \Leftrightarrow\ & A_i^\dagger A_i\rho A_j^\dagger A_j = 0 \\ \Rightarrow\ & (A_i^\dagger)^- A_i^\dagger A_i\rho A_j^\dagger A_j A_j^- = 0 \\ \Leftrightarrow\ & \Pi_{\text{im}\,A_i} A_i\rho A_j^\dagger \Pi_{\text{supp}\,A_j^\dagger} = 0 \\ \Leftrightarrow\ & A_i\rho A_j^\dagger = 0. \end{aligned} \tag{D4}$$

Since $C_{\text{rel}}(\rho,\mathbf{E})$ is independent of the choice of Naimark extension, we thus obtain a general characterization of POVM-incoherent states. □

• *Proof of* **Lemma 2** *from main text.* According to Prop. 5, a state ρ is POVM-incoherent iff $E_i\rho E_j = 0$ for all $i \neq j$. This implies that $\rho = (\sum_i E_i)\rho(\sum_j E_j) = \sum_i E_i\rho E_i$. Thus, we obtain the following necessary condition for a POVM-incoherent state

$$\text{tr}[\sum_i E_i^2\rho] = 1. \tag{D5}$$

This equation can only be fulfilled if $\sum_i E_i^2|_{\text{supp}\,\rho} = \mathbb{1}$. On the other hand, due to normalization also $\sum_i E_i|_{\text{supp}\,\rho} = \mathbb{1}$ holds. This means that any POVM-incoherent state can only have support on the projective parts $\bar{E}_i$ of the E_i. Moreover, due to the characterization from Prop. 5, an incoherent state ρ cannot possess coherence across the subspaces stabilized by the $\bar{E}_i$. Therefore, we obtain the following characterization: any POVM-incoherent state needs to fulfill

$$\sum_i \bar{E}_i\rho_{\text{PI}}\bar{E}_i = \rho_{\text{PI}}, \text{ or equivalently,} \tag{D6}$$

$$\rho_{\text{PI}} = \oplus_i p_i\sigma_i, \tag{D7}$$

where $\{p_i\}$ is a probability distribution and σ_i a quantum state with $\text{supp}\,\sigma_i = \text{supp}\,\bar{E}_i$. We can immediately verify the condition from Prop. 5 for this expression. Since $\bar{E}_k$ is a projector, any other effect $E_{i\neq k}$ (projective or not) must necessarily have orthogonal support, otherwise normalization cannot be achieved. Thus,

$$E_i\rho_{\text{PI}}E_j = \sum_k E_i(\bar{E}_k\rho_{\text{PI}}\bar{E}_k)\bar{E}_j = 0 \quad \forall i\neq j. \tag{D8}$$

□

As a corollary we obtain that for any POVM for which no effect has a projective part the set of POVM-incoherent states of $\mathbf{E}$ is empty. This shows that there can be a finite gap between the set of embedded states $\mathcal{S}_\mathcal{E} \subseteq \mathcal{S}'$ and the set of block-incoherent states $\mathcal{I} \subseteq \mathcal{S}'$.

Since POVM-incoherent states do not exist for all measurements, it is important to characterize states with minimal and maximal POVM-based coherence. The measure $C_{\text{rel}}(\rho,\mathbf{E})$ is bounded by the extremal values of the corresponding block-coherence measure on $\mathcal{S}'$ given by $0 \leq C(\rho',\mathbf{P}) \leq \log(d')$. However, the upper bound can be made tighter.

Proposition 6. Let $\mathbf{E}$ be an n-outcome POVM. The POVM-based coherence measure $C_{\text{rel}}(\rho,\mathbf{E})$ satisfies the bounds $0 \leq C_{\text{rel}}(\rho,\mathbf{E}) \leq \log n$.

Proof. We show the upper bound. First, we consider the pure state case $\rho = |\psi\rangle\langle\psi|$, for which the measure reads

$$C_{\text{rel}}(|\psi\rangle, \mathbf{E}) = H(\{p_i(|\psi\rangle)\}). \tag{D9}$$

The expression is maximized for states with uniform outcomes $p_i = \frac{1}{n}$ which yields $H(\{p_i(|\psi\rangle)\}) \leq \log n$. Since $C_{\text{rel}}(\rho, \mathbf{E})$ is a convex function, i.e., it decreases under mixing, the maxima are attained by pure states, and thus $C_{\text{rel}}(\rho, \mathbf{E}) \leq \log n$ also holds for mixed states. □

The convexity of C_{rel} implies that the maximum coherence of a POVM is attained by the pure states with highest outcome entropy. However, analytically maximizing C_{rel} even for pure states is generally hard, see e.g., Ref. [10], where the maximal value for all symmetric informationally complete (SIC-) POVMs was obtained. Examples for POVMs that attain the upper bound of $\log n$ are the qubit trine POVM, but also informationally complete POVMs, namely those for which there are pure states with maximal randomness gain [11]. Moreover, one can readily construct rank-one POVMs in any dimension that achieve the upper bound.

Finally, we discuss states which minimize C_{rel} for a given POVM. Because C_{rel} is a convex function on a convex set it can be shown that the set $\mathcal{M}$ of its minima is convex. In the qubit case, the states with minimal coherence can be found analytically. Qubit quantum states can be parameterized as $\rho(\vec{r}) = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma})$ with Bloch vector $|\vec{r}| \leq 1$, and $\vec{r}\cdot\vec{\sigma} = \sum_i r_i\sigma_i$, where σ_i denotes the i-th Pauli matrix. The function $\rho(\vec{r})$ is affine in $\vec{r}$ and thus $C_{\text{rel}}(\vec{r}) \coloneqq C_{\text{rel}}(\rho(\vec{r}))$ is convex. Consequently, for any fixed POVM $\mathbf{E}$ we have the following optimization problem

$$\begin{aligned} &\text{minimize} && C_{\text{rel}}(\vec{r}) \\ &\text{such that} && |\vec{r}|^2 - 1 \leq 0 \end{aligned} \tag{D10}$$

This is a convex optimization problems, i.e., the objective function $C_{\text{rel}}(\vec{r})$ and the inequality contraint function $g(\vec{r}) = |\vec{r}|^2 - 1$ are convex. For such problems it is known that any point $\vec{r}^*$ that fulfills the Karush–Kuhn–Tucker (KKT) [12] conditions is a global minimum of the objective function. One can readily check that for the problem above a point $\vec{r}^*$ fulfills the KKT conditions if

$$|\vec{r}^*|^2 \leq 1 \quad \text{and} \quad \nabla_{\vec{r}} C_{\text{rel}}(\vec{r}^*) = 0. \tag{D11}$$

Therefore, given a POVM $\mathbf{E}$, the minimum of $C_{\text{rel}}(\rho, \mathbf{E})$ is achieved for states $\rho(\vec{r}^*)$ with $\vec{r}^*$ from Eq. (D11). In dimensions higher than two, a similar analysis can be carried out with more involved constraints.

Appendix E: POVM-incoherent operations

In this part, we provide proofs for the general results concerning POVM-incoherent operations from the main text. In particular, we present the semidefinite programs that characterize the set of POVM-incoherent operations and the fidelity $F_{\max}(\rho, \sigma)$, respectively.

• *Proof of* **Lemma 3** *from main text.* Let Λ_{MPI} be a POVM-incoherent operation with respect to the POVM $\mathbf{E}$. By definition there exists a channel Λ'_{MBI} on $\mathcal{S}'$ obeying the two properties from Def. 2 such that $\Lambda_{\text{MPI}}[\rho] \oplus 0 = \Lambda'_{\text{MBI}}[\rho \oplus 0]$. Thus, it holds that

$$\begin{aligned} C(\Lambda_{\text{MPI}}[\rho], \mathbf{E}) &= C(\Lambda_{\text{MPI}}[\rho] \oplus 0, \mathbf{P}) \\ &= C(\Lambda'_{\text{MBI}}[\rho \oplus 0], \mathbf{P}) \\ &\leq C(\rho \oplus 0, \mathbf{P}) = C(\rho, \mathbf{E}), \end{aligned} \tag{E1}$$

where the inequality is a consequence of Λ'_{MBI} being an block-incoherent operation with respect to $\mathbf{P}$. □

If the Naimark space has tensor product form $\mathcal{H} \otimes \mathcal{H}_R$, then due to subspace-preservation Λ' can be decomposed as

$$\begin{aligned} \Lambda' &= \Omega \circ \Lambda' \circ \Omega + \Lambda' \circ \Omega^\perp \\ &= (\Lambda \otimes \text{id}) \circ \Omega + \Lambda' \circ \Omega^\perp, \end{aligned} \tag{E2}$$

where Λ is a channel on $\mathcal{S}$, $\Omega[\rho'] = \Pi_\mathcal{E}\rho'\Pi_\mathcal{E}$ and $\Omega^\perp = \text{id} - \Omega$. Thus, in this case we have $\Lambda'|_{\mathcal{S}_\mathcal{E}} = \Lambda \otimes \text{id}$, leading to the local operation Λ on $\mathcal{S}$.

In the following, we show that the set of POVM-incoherent operations of a POVM $\mathbf{E}$ is independent of the choice of Naimark extension used for its definition. We consider any Naimark extension $\mathbf{P}$ of $\mathbf{E}$ as defined in Eq. (1), not necessarily of tensor product form. For that, it is instructive to read the proof of Lemma 1 established in App. C. There, we summarized the generalized embedding definitions introduced in App. A,

$$\mathcal{E}[X] = X \oplus 0, \quad \mathcal{H}_\mathcal{E} = \{|\psi\rangle \oplus 0\}, \quad \Pi_\mathcal{E} = \mathbb{1} \oplus 0. \tag{E3}$$

• *Proof of* **Theorem 1** *from main text.* First, we prove that the set of POVM-incoherent operations is independent of the choice of Naimark extension used for its definition. We start by showing some useful relations that connect different Naimark extensions of a POVM. Let $\mathbf{P}$, $\hat{\mathbf{P}}$ be two Naimark extensions of the same POVM $\mathbf{E}$ such that $\operatorname{rank}\hat{P}_i \leq \operatorname{rank} P_i$. Let the effects of the extensions have spectral decomposition $P_i = \sum_k |i,k\rangle\langle i,k|$ and $\hat{P}_i = \sum_{\hat{k}} |i,\hat{k}\rangle\langle i,\hat{k}|_S$ (S for small), respectively. Define the partial isometry $Q^\dagger$ as

$$Q^\dagger|i,k\rangle = \begin{cases} |i,k\rangle_S & \text{for } k = \hat{k} = 1,\ldots,\operatorname{rank}\hat{P}_i \\ 0 & \text{for } k > \operatorname{rank}\hat{P}_i. \end{cases} \tag{E4}$$

Consequently, the operator Q is an isometry which satisfies

$$\begin{aligned} P_i Q &= \sum_k |i,k\rangle\langle i,k|Q = \sum_{\hat{k}} |i,\hat{k}\rangle\langle i,\hat{k}|_S \\ Q\hat{P}_i &= \sum_{\hat{k}} Q|i,\hat{k}\rangle_S\langle i,\hat{k}|_S = \sum_{\hat{k}} |i,\hat{k}\rangle\langle i,\hat{k}|_S. \end{aligned} \tag{E5}$$

This implies that

$$\begin{aligned} &P_i Q = Q\hat{P}_i \quad \text{and} \\ &\mathcal{Q}\circ\hat{\Delta} = \Delta\circ\mathcal{Q}, \end{aligned} \tag{E6}$$

where we have defined the isometric channel $\mathcal{Q}[\rho_S] = Q\rho_S Q^\dagger$. Therefore, the two Naimark extension can be related as

$$\hat{P}_i = Q^\dagger Q\hat{P}_i = Q^\dagger P_i Q, \tag{E7}$$

which ensures that $\hat{P}_i$ is normalized: $\sum_i Q^\dagger P_i Q = Q^\dagger \mathbb{1} Q = \mathbb{1}$.

Since $\mathbf{P}$, $\hat{\mathbf{P}}$ are Naimark extensions of the same POVM $\mathbf{E}$, the isometry Q can be further constrained. It holds that $\Pi_\mathcal{E} P_i \Pi_\mathcal{E} = \Pi_\mathcal{E} \hat{P}_i \Pi_\mathcal{E} = \mathcal{E}[E_i]$, and therefore

$$\begin{aligned} &\Pi_\mathcal{E} P_i \Pi_\mathcal{E} = \Pi_\mathcal{E} Q^\dagger P_i Q \Pi_\mathcal{E} \\ \Leftrightarrow\ &(P_i \Pi_\mathcal{E})^\dagger (P_i \Pi_\mathcal{E}) = (P_i Q \Pi_\mathcal{E})^\dagger (P_i Q \Pi_\mathcal{E}). \end{aligned} \tag{E8}$$

For relations of the form $A_i^\dagger A_i = B_i^\dagger B_i$ it holds that $B_i = U_i A_i$ [13] with U_i being a unitary. In our case we have $A_i = P_i \Pi_\mathcal{E}$ and $B_i = P_i Q \Pi_\mathcal{E}$, that is,

$$P_i Q \Pi_\mathcal{E} = U_i P_i \Pi_\mathcal{E}. \tag{E9}$$

Define the operator

$$C_i = P_i Q \Pi_\mathcal{E} (P_i \Pi_\mathcal{E})^-, \tag{E10}$$

where X^- denotes the generalized (Moore-Penrose) inverse of any operator X [9]. From Eq. (E9) we see that the matrix $C_i = U_i P_i \Pi_\mathcal{E} (P_i \Pi_\mathcal{E})^- = U_i \tilde{P}_i$, where $P_i = \tilde{P}_i + \tilde{P}_i^\perp$, is a partial isometry since $C_i^\dagger C_i = \tilde{P}_i$ is a projector. Note that $\operatorname{supp} C_i \subseteq \pi_i$ and $\operatorname{im} C_i \subseteq \pi_i$, where π_i denotes the image of P_i. This means that the restriction $C_i|_{\pi_i} : \pi_i \to \pi_i$ is a partial isometry, too. Therefore $C_i|_{\pi_i}$ can be extended to an isometry $\bar{C}_i : \pi_i \to \pi_i$ with *full* support on π_i by defining:

$$\bar{C}_i := \begin{cases} C_i|_{\pi_i} & \text{on } \operatorname{supp} C_i|_{\pi_i} \\ \mathbb{1} & \text{on } \ker C_i|_{\pi_i} \end{cases}, \tag{E11}$$

which is equivalent to $\bar{C}_i = (U_i \tilde{P}_i + \tilde{P}_i^\perp)|_{\pi_i}$. Then we introduce

$$U := \oplus_i \bar{C}_i \tag{E12}$$

which is a block-diagonal unitary operator since

$$U^\dagger U = \oplus_{i,j} \bar{C}_i^\dagger \bar{C}_j = \oplus_i \bar{C}_i^\dagger \bar{C}_i = \sum_i P_i = \mathbb{1}. \tag{E13}$$

With that, we can write Eq. (E9) as

$$P_i Q \Pi_\mathcal{E} = U P_i \Pi_\mathcal{E}. \tag{E14}$$

By summing over i, we obtain

$$\begin{aligned} &Q \Pi_\mathcal{E} = U \Pi_\mathcal{E} \quad \text{and} \\ &\mathcal{Q} \circ \mathcal{E} = \mathcal{U} \circ \mathcal{E}. \end{aligned} \tag{E15}$$

Finally, since the unitary is block-diagonal it commutes with the Naimark extension effects

$$\begin{aligned} &U P_i = P_i U \quad \text{and} \\ &\Delta \circ \mathcal{U} = \mathcal{U} \circ \Delta. \end{aligned} \tag{E16}$$

The channel $\mathcal{Q}^\dagger[\rho] = Q^\dagger \rho Q$ is completely positive but generally not trace-preserving. For this we define the projector $S := QQ^\dagger$ and its complement $S^\perp = \mathbb{1} - S$. It holds that $\Delta[S] = \sum_i P_i Q Q^\dagger P_i = \sum_i Q \hat{P}_i Q^\dagger = S$ and also $\Delta[S^\perp] = S^\perp$. We define the map

$$\mathcal{T}[\rho] := \operatorname{tr}(S^\perp \rho) \mathbb{1} / d_{\min} \tag{E17}$$

which crucially satisfies

$$\hat{\Delta} \circ \mathcal{T}[\rho] = \operatorname{tr}(S^\perp \rho) \hat{\Delta}[\mathbb{1}] / d_{\min} = \mathcal{T}[\rho], \tag{E18}$$

and also

$$\begin{aligned} \mathcal{T} \circ \Delta[\rho] &= \operatorname{tr}(S^\perp \Delta[\rho]) \mathbb{1} / d_{\min} \\ &= \operatorname{tr}(\Delta[S^\perp] \rho) \mathbb{1} / d_{\min} = \mathcal{T}[\rho]. \end{aligned} \tag{E19}$$

Now we are able to define the following *reversal* channel of the isometric channel $\mathcal{Q}$

$$\mathcal{R} = \mathcal{Q}^\dagger + \mathcal{T}. \tag{E20}$$

It holds that $\mathcal{R} \circ \mathcal{Q}[\rho] = \rho$. Moreover, one can check that $\mathcal{R}$ is completely positive and trace-preserving: $\operatorname{tr}(\mathcal{R}[\rho]) = \operatorname{tr}(S\rho) + \operatorname{tr}(S^\perp \rho) = \operatorname{tr}(\rho) = 1$. By combining the Eqs. (E6), (E18), (E19) we observe that the following equation holds

$$\hat{\Delta} \circ \mathcal{R} = \mathcal{R} \circ \Delta. \tag{E21}$$

Finally, it holds that $\mathcal{T} \circ \mathcal{E}[\rho] = \operatorname{tr}(S^\perp \mathcal{E}[\rho]) \mathbb{1} / d_{\min} = 0$ and therefore

$$\mathcal{R} \circ \mathcal{E} = \mathcal{Q}^\dagger \circ \mathcal{E}. \tag{E22}$$

Having established the above relations, we come to the main independence proof. Let Γ be any block-incoherent (MBI) and subspace-preserving (SP) map with respect to $\mathbf{P}$. We define the map $\hat{\Gamma} := \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{Q}$ which acts on states of the smaller Naimark space. Clearly, $\hat{\Gamma}$ is completely positive and trace-preserving, as it is the concatenation of channels. We show below that $\hat{\Gamma}$

1. is block-incoherent with respect to $\hat{\mathbf{P}}$,
2. is subspace-preserving,
3. leads to the same POVM-incoherent operation as Γ.

For the first claim, we verify that $\hat{\Gamma}$ is block-incoherent with respect to $\hat{\mathbf{P}}$, i.e., $\hat{\Delta} \circ \hat{\Gamma} \circ \hat{\Delta} = \hat{\Delta} \circ \hat{\Gamma}$ holds:

$$\begin{aligned} \hat{\Delta} \circ \hat{\Gamma} \circ \hat{\Delta} &= \hat{\Delta} \circ \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{Q} \circ \hat{\Delta} \\ &= \mathcal{R} \circ \Delta \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \Delta \circ \mathcal{Q} \\ &= \mathcal{R} \circ \mathcal{U} \circ \Delta \circ \Gamma \circ \Delta \circ \mathcal{U}^\dagger \circ \mathcal{Q} \\ &= \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \Delta \circ \mathcal{U}^\dagger \circ \mathcal{Q} \\ &= \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \Delta \circ \mathcal{Q} \\ &= \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{Q} \circ \hat{\Delta} \\ &= \hat{\Gamma} \circ \hat{\Delta}. \end{aligned} \tag{E23}$$

In the fourth equation we have used that Γ is MBI w.r.t. $\mathbf{P}$.

For the second claim, we verify that $\hat{\Gamma}$ is subspace-preserving, i.e., $\Omega \circ \hat{\Gamma} \circ \Omega = \hat{\Gamma} \circ \Omega$, where $\Omega = \mathcal{E} \circ \mathcal{E}^\dagger$:

$$\begin{aligned} \hat{\Gamma} \circ \Omega &= \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{Q} \circ \Omega \\ &= \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{U} \circ \Omega \\ &= \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \Omega \circ \mathcal{U}^\dagger \circ \mathcal{U} \\ &= \mathcal{R} \circ \mathcal{U} \circ \Omega \circ \Gamma \circ \Omega \circ \mathcal{U}^\dagger \circ \mathcal{U} \\ &= \Omega \circ \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{Q} \circ \Omega \\ &= \Omega \circ \hat{\Gamma} \circ \Omega \end{aligned} \tag{E24}$$

In the fourth equation we have used that Γ is subspace-preserving.

Finally, for the third claim we show that $\hat{\Gamma}$ leads to the same POVM-incoherent operation as Γ. By using

- that Γ is subspace-preserving: $\Gamma \circ \mathcal{E} = \Omega \circ \Gamma \circ \mathcal{E}$,
- $\mathcal{R} \circ \mathcal{U} \circ \Omega = \mathcal{R} \circ \mathcal{Q} \circ \Omega = \Omega$,

we see that the following holds:

$$\begin{aligned}\mathcal{E}^\dagger \circ \hat{\Gamma} \circ \mathcal{E} &= \mathcal{E}^\dagger \circ \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{Q} \circ \mathcal{E} \\ &= \mathcal{E}^\dagger \circ \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{U} \circ \mathcal{E} \\ &= \mathcal{E}^\dagger \circ \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{E} \\ &= \mathcal{E}^\dagger \circ \mathcal{R} \circ \mathcal{U} \circ \Omega \circ \Gamma \circ \mathcal{E} \\ &= \mathcal{E}^\dagger \circ \Gamma \circ \mathcal{E}. \end{aligned} \tag{E25}$$

Altogether, we conclude that the set of POVM-incoherent operations is well-defined as it does not depend on the choice of Naimark extension for its definition.

With the independence property established in the previous paragraph we can show that if $\mathbf{E}$ is an orthogonal rank-1 measurement, POVM-incoherent operations MPI are equivalent to coherence MIO channels. Since in this case $\mathbf{E}$ is already projective, we can choose the trivial Naimark space $\mathcal{H}' = \mathcal{H} \otimes \mathbb{C} \simeq \mathcal{H}$ and $\mathbf{P} = \mathbf{E}$. Then, subspace-preservation is trivially fulfilled for all channels from $\mathcal{S}$ to itself, while the block-incoherent condition is equivalent to the MIO condition in standard coherence theory. Since POVM-incoherent operations are independent of the chosen Naimark extension the assertion also holds for any other Naimark extension of $\mathbf{E}$.

Finally, we show that the set of POVM-incoherent operations can be characterized by a semidefinite program. Let $\mathcal{B} = \{B_\alpha\}_\alpha = \{|i\rangle\langle j|\}_{i,j=1}^{d'}$ be the (Hilbert-Schmidt-orthonormal) standard matrix basis of operators on $\mathcal{H}'$ in lexicographical order. Let $\mathrm{vec} : \mathcal{S}' \to \mathbb{C}^{d'^2}$ be the isomorphism that maps a state ρ on the Naimark space to its coordinate vector $\mathrm{vec}(\rho)$ with respect to $\mathcal{B}$. To any superoperator Λ' on $\mathcal{S}'$, we associate its coordinate matrix with respect to $\mathcal{B}$, called the process matrix,

$$\hat{\Lambda}'_{\alpha,\beta} = \mathrm{tr}[B_\alpha^\dagger \Lambda'[B_\beta]], \tag{E26}$$

which has the property that $\hat{\Lambda}' \mathrm{vec}(\rho) = \mathrm{vec}(\Lambda'[\rho])$ [14]. The process matrix $\hat{\Lambda}'$ is related to the Choi matrix $J_{\Lambda'}$ of Λ' as [14]

$$\hat{\Lambda}' = d' J^R_{\Lambda'}, \quad X^R := \sum_\alpha (\mathbb{1} \otimes B_\alpha) X (B_\alpha \otimes \mathbb{1}), \tag{E27}$$

where the mapping $X \to X^R$ is an involution, called row-reshuffling [15]. On the level of transfer matrices the composition of superoperators $\mathcal{E} \circ \mathcal{F}$ becomes multiplication $\hat{\mathcal{E}}\hat{\mathcal{F}}$. With that we can characterize POVM incoherent operations via a semidefinite feasibility problem. A system channel Λ on $\mathcal{S}$ is POVM-incoherent if and only if there exists a Choi matrix J on $\mathcal{H}' \otimes \mathcal{H}'$ such that

$$\begin{aligned} \text{find:} \quad & d' \hat{\mathcal{E}}^\dagger J^R \hat{\mathcal{E}} = \hat{\Lambda} \\ \text{subj. to:} \quad & J \geq 0, \quad \mathrm{tr}_1 J = \tfrac{\mathbb{1}}{d'}, \\ & J^R \hat{\Delta} = \hat{\Delta} J^R \hat{\Delta}, \\ & J^R \hat{\Omega} = \hat{\Omega} J^R \hat{\Omega}. \end{aligned} \tag{E28}$$

Here tr_1 denotes the trace over the first subsystem of $\mathcal{H}' \otimes \mathcal{H}'$, and $\mathcal{E}[\rho] = \rho \oplus 0$. Moreover, Δ denotes the block-dephasing operator and $\Omega[\rho'] := \Pi_\mathcal{E} \rho' \Pi_\mathcal{E}$, with $\Pi_\mathcal{E}$ being the projector onto $\mathcal{S}_\mathcal{E}$. The SDP characterization allows for an efficient numerical check whether a channel is element of the set of POVM-incoherent operations. □

The fidelity between two quantum states ρ, σ is given by $F(\rho,\sigma) = \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$. We define the quantity $F_{\max}(\rho,\sigma) = \max_{\Lambda_{\mathrm{MPI}}} F(\Lambda_{\mathrm{MPI}}[\rho], \sigma)$ between the states σ and $\Lambda_{\mathrm{MPI}}[\rho]$, maximized over all POVM-incoherent operations Λ_{MPI} of a POVM $\mathbf{E}$. The quantity characterizes the usefulness of a particular state ρ when only POVM-incoherent operations can be implemented, as it provides a measure of how well σ can be approximated. As a consequence of the SDP characterization of POVM-incoherent operations we are able to efficiently numerically calculate $F_{\max}$.

Proposition 7. The fidelity $F_{\max}(\rho,\sigma) = \max F(\Lambda_{\mathrm{MPI}}[\rho], \sigma)$ equals the solution of the following semidefinite program

$$\begin{aligned} & F_{\max}(\rho,\sigma) = \\ \text{maximize:} \quad & \frac{1}{2}(\mathrm{tr}[X] + \mathrm{tr}[X^\dagger]) \\ \text{subj. to:} \quad & \begin{pmatrix} \sigma & X \\ X^\dagger & \Lambda[\rho] \end{pmatrix} \geq 0, \\ & \Lambda[\rho] = \mathrm{vec}^{-1}(d' \hat{\mathcal{E}}^\dagger J^R \hat{\mathcal{E}}\, \mathrm{vec}(\rho)) \\ & J \geq 0, \quad \mathrm{tr}_1 J = \tfrac{\mathbb{1}}{d'}, \\ & J^R \hat{\Delta} = \hat{\Delta} J^R \hat{\Delta}, \\ & J^R \hat{\Omega} = \hat{\Omega} J^R \hat{\Omega}. \end{aligned} \tag{E29}$$

Proof. The fidelity between two arbitrary quantum states can be cast in the form of an SDP [16, 17]. Combining this with the SDP characterization of POVM-incoherent operations from the proof of Theorem 1 proves the assertion. □

Appendix F: Example: qubit trine POVM

In this section we apply all previously obtained results to study the POVM-based coherence theory of qubit POVMs.

Coherence theory of mixed-unitary channel

The simplest example for a POVM-based coherence theory is obtained from the Kraus operators of a mixed-unitary channel which lead to the POVM $\mathbf{E} = \{p_1\mathbb{1}, \ldots, p_n\mathbb{1}\}$ with a probability distribution $\{p_i\}$. The canonical Naimark extension is given by $\mathbf{P} = \{\mathbb{1} \otimes |\varphi_i\rangle\langle\varphi_i|\}$, where $|\varphi_i\rangle$ is an orthonormal basis of $\mathcal{H}_R$ such that $|\langle\varphi_i|1\rangle|^2 = p_i$. In this case all states have the same coherence of $C_{\mathrm{rel}}(\rho, \mathbf{E}) = H(\{p_i\})$, since the system-apparatus interaction is just a local unitary generating coherence in the measurement apparatus. As a consequence all system channels Λ on $\mathcal{S}$ are POVM-incoherent, since the embedding $\Lambda \otimes \mathrm{id}$ is subspace-preserving and commutes with the dephasing operation $\Delta[\cdot] = \sum_i P_i \cdot P_i$ and thus maps incoherent states to themselves, $(\Lambda \otimes \mathrm{id})[\Delta[\rho]] = \Delta[(\Lambda \otimes \mathrm{id})[\rho]]$. Note that in general

a part of this coherence is used to generate classical randomness for the mixing of the POVM. If the experimenter is able to perform statistical mixtures of measurements, certain POVMs can be implemented with less resource. However, this is not the case for extremal measurements [18].

Coherence theory of qubit trine POVM

In this section we apply the results from the main text to study the POVM-based coherence theory of the qubit trine POVM which is given by

$$\mathbf{E} = \left\{\frac{1}{3}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}, \frac{1}{3}\begin{pmatrix}1 & \omega^*\\ \omega & 1\end{pmatrix}, \frac{1}{3}\begin{pmatrix}1 & \omega\\ \omega^* & 1\end{pmatrix}\right\}, \tag{F1}$$

with $\omega = e^{\frac{2\pi}{3}i}$, and $\omega^* = \omega^2$. Since our resource theory is independent of the choice of Naimark extension, it is numerically advantageous to employ the Naimark extension of smallest dimension. Such a minimal Naimark extension of $\mathbf{E}$ is given by $\mathbf{P} = \{|\varphi_i\rangle\langle\varphi_i|\}_{i=1}^3$ on $\mathcal{H}' = \mathbb{C}^3$ with

$$|\varphi_1\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |2\rangle + |3\rangle) \tag{F2}$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{3}}(|1\rangle + \omega|2\rangle + \omega^*|3\rangle) \tag{F3}$$

$$|\varphi_3\rangle = \frac{1}{\sqrt{3}}(|1\rangle + \omega^*|2\rangle + \omega|3\rangle. \tag{F4}$$

Any incoherent state on $\mathcal{S}'$ with respect to $\mathbf{P}$ can be written as

$$\rho_I = \sum_i^3 p_i|\varphi_i\rangle\langle\varphi_i| = \frac{1}{3}\begin{pmatrix}1 & p_1+\omega^* p_2+\omega p_3 & p_1+\omega p_2+\omega^* p_3\\ p_1+\omega p_2+\omega^* p_3 & 1 & p_1+\omega^* p_2+\omega p_3\\ p_1+\omega^* p_2+\omega p_3 & p_1+\omega p_2+\omega^* p_3 & 1\end{pmatrix}, \tag{F5}$$

for some probability distribution $\{p_i\}_{i=1}^3$. Moreover, a general embedded system state in $\mathcal{S}_\mathcal{E} \subseteq \mathcal{S}'$ is of the form

$$\mathcal{E}[\rho] = \rho \oplus 0 = \begin{pmatrix}\rho_{11} & \rho_{12} & 0\\ \rho_{21} & \rho_{22} & 0\\ 0 & 0 & 0\end{pmatrix}, \tag{F6}$$

with $\rho \in \mathcal{S}$. Finally, any dephased embedded state reads as

$$\Delta[\rho \oplus 0] = \frac{1}{3}\begin{pmatrix}1 & \rho_{12} & \rho_{21}\\ \rho_{21} & 1 & \rho_{12}\\ \rho_{12} & \rho_{21} & 1\end{pmatrix}. \tag{F7}$$

We now provide a characterization of the POVM-incoherent unitaries of the trine POVM. Let U' be a unitary on the Naimark space $\mathcal{H}' = \mathbb{C}^3$ that is

i. *(Naimark-) incoherent:* $U'|\varphi_i\rangle \propto |\varphi_j\rangle$

ii. *Subspace-preserving:* $U'\begin{pmatrix}|\psi\rangle\\ 0\end{pmatrix} = \begin{pmatrix}|\psi'\rangle\\ 0\end{pmatrix}$,

with $|\psi\rangle, |\psi'\rangle \in \mathbb{C}^2$ and $|\varphi_i\rangle$ being the i-th measurement vector of the Naimark extension. Then we call the operator U^{trine} on $\mathcal{H} = \mathbb{C}^2$ given by

$$U^{\text{trine}} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} U' \begin{pmatrix}1 & 0\\ 0 & 1\\ 0 & 0\end{pmatrix} \tag{F8}$$

a POVM-incoherent unitary of the trine POVM. It has been shown [19] that all qutrit incoherent unitaries are of the form

$$U'_\pi = \sum_{i=1}^3 e^{i\alpha_i}|\varphi_{\pi(i)}\rangle\langle\varphi_i|, \tag{F9}$$

where $\alpha_i \in \mathbb{R}$ and $\pi = (\pi(1)\ \pi(2)\ \pi(3)) \in S_3$ is one of the six permutations of a three-element set. Thus, there are six classes of 3-parameter incoherent unitaries. Moreover, the subspace-preservation condition ii. is fulfilled for all $|\psi\rangle \in \mathbb{C}^2$ if and only if the unitary is of the form

$$U'_\pi = \begin{pmatrix}* & * & *\\ * & * & *\\ 0 & 0 & *\end{pmatrix}, \tag{F10}$$

where $*$ denotes some complex entry. Therefore, to obtain a POVM-incoherent unitary we require that U'_π satisfies $(U'_\pi)_{3,1} = (U'_\pi)_{3,2} = 0$. This yields the POVM-incoherent unitary U^{trine} as the upper left 2×2 block of the resulting matrix. The following list contains all trine POVM-incoherent unitaries:

$$\begin{aligned}
U^{\text{trine}}_{(123)} &= \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \mathbb{1},\\
U^{\text{trine}}_{(231)} &= \begin{pmatrix}\sqrt{\omega^*} & 0\\ 0 & \sqrt{\omega}\end{pmatrix} = R_{\vec{e}_z}(\frac{2\pi}{3}),\\
U^{\text{trine}}_{(312)} &= \begin{pmatrix}\omega^* & 0\\ 0 & \omega\end{pmatrix} = R_{\vec{e}_z}(\frac{4\pi}{3}),\\
U^{\text{trine}}_{(132)} &= \begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix} = R_{\vec{m}_1}(\pi),\\
U^{\text{trine}}_{(321)} &= \begin{pmatrix}0 & \omega^{\frac{5}{4}}\\ \omega^{\frac{1}{4}} & 0\end{pmatrix} = R_{\vec{m}_2}(\pi),\\
U^{\text{trine}}_{(213)} &= \begin{pmatrix}0 & \omega^{\frac{1}{4}}\\ \omega^{\frac{5}{4}} & 0\end{pmatrix} = R_{\vec{m}_3}(\pi),
\end{aligned} \tag{F11}$$

Up to a phase, any qubit unitary can be expressed as $R_{\vec{n}}(\theta) = e^{-i\frac{\theta}{2}\vec{n}\cdot\vec{\sigma}} \in \mathrm{SU}(2)$, namely as the rotation around the bloch vector $\vec{n}$ with angle θ. Here, $\vec{m}_i$ denotes the Bloch vector of the measurement vector $|\varphi_i\rangle$, and U^{trine}_π denotes the POVM-incoherent unitary obtained from U'_π. This set is composed of the six rotations that leave the equilateral triangle, whose vertices are given by the measurement direction vectors $\{\vec{m}_i\}$, invariant. There are no continuous degrees of freedom left, since the two subspace-preserving conditions together with the requirement of having unit determinant uniquely determines the parameters α_i.

At last, we discuss the usefulness of a maximally coherent state $|\Psi_\text{m}\rangle \in \{|0\rangle, |1\rangle\}$ for the POVM-based coherence theory of the trine POVM. We have numerical evidence that the transformation $|\Psi_\text{m}\rangle\langle\Psi_\text{m}| \to \rho$ with $\rho \in \mathcal{S}$ is always possible by a maximally

POVM-incoherent (MPI) map. Concretely, by plotting the value of $F_{\max}(|\Psi_{\mathrm{m}}\rangle, \sigma)$ for any pure state $\sigma = |\psi\rangle\langle\psi|$, we observe that all pure states can be obtained with certainty from $|\Psi_{\mathrm{m}}\rangle$ under POVM-incoherent operations. Therefore, all qubit states $\rho = \sum_i p_i |i\rangle\langle i|$ can be obtained from $|\Psi_{\mathrm{m}}\rangle$ by a POVM-incoherent map, namely via preparing the eigenstate $|i\rangle$ with probability p_i.

[1] J. Åberg, arXiv:quant-ph/0612146 (2006).
[2] P.-X. Chen, J. A. Bergou, S.-Y. Zhu, and G.-C. Guo, Physical Review A **76**, 060303(R) (2007).
[3] A. Streltsov, G. Adesso, and M. B. Plenio, Reviews of Modern Physics **89**, 041003 (2017).
[4] T. Baumgratz, M. Cramer, and M. B. Plenio, Physical Review Letters **113**, 140401 (2014).
[5] V. Vedral and M. B. Plenio, Physical Review A **57**, 1619 (1998).
[6] J. Matera, D. Egloff, N. Killoran, and M. B. Plenio, Quantum Science and Technology **1**, 01LT01 (2016).
[7] E. Chitambar, A. Streltsov, S. Rana, M. N. Bera, G. Adesso, and M. Lewenstein, Physical Review Letters **116**, 070402 (2016).
[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[9] J. C. A. Barata and M. S. Hussein, Brazilian Journal of Physics **42**, 146 (2012).
[10] A. Szymusiak, arXiv:1701.01139 (2017).
[11] F. Bischof, H. Kampermann, and D. Bruß, Physical Review A **95**, 062305 (2017).
[12] S. Boyd and L. Vandenberghe, *Convex optimization* (Cambridge University Press, 2004).
[13] N. J. Higham, C. Mehl, and F. Tisseur, SIAM Journal on Matrix Analysis and Applications **31**, 2163 (2010).
[14] T. F. Havel, Journal of Mathematical Physics **44**, 534 (2003).
[15] C. J. Wood, J. D. Biamonte, and D. G. Cory, Quantum Information & Computation **15**, 0579 (2015).
[16] M. Piani, Physical Review Letters **117**, 080401 (2016).
[17] J. Watrous, arXiv:1207.5726 (2012).
[18] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Physical Review Letters **119**, 190501 (2017).
[19] Z. Bai and S. Du, Quantum Information & Computation **15**, 1355 (2015).

A.3 Quantifying coherence with respect to general quantum measurements

Title:	Quantifying coherence with respect to general quantum measurements
Authors:	Felix Bischof, Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review A
Impact factor:	2.907 (2018)
Date of submission:	05 August 2019
Publication status:	Under Review
Contribution by F.B.:	First author (input approx. 90%)

This publication corresponds to the Bibliography entry [BKB19]. A summary of the results is given in Sec. 7.4. The main ideas and research objectives were devised by me. I derived the connection of POVM-based coherence to randomness generation. Moreover, I investigated the probabilistic resource-theoretical framework and proved its consistency. In addition, I provided the resource measures and established the connections among them in collaboration with my co-authors. The example based on the qubit trine POVM was analyzed by me. I performed all numerical computations and created the figures and plots. Finally, I prepared the manuscript and gave the bibliography concerning the state of the art.

Quantifying coherence with respect to general quantum measurements

Felix Bischof,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany
(Dated: August 16, 2019)

Coherence is a cornerstone of quantum theory and a prerequisite for the advantage of quantum technologies. In recent work, the notion of coherence with respect to a general quantum measurement (POVM) was introduced and embedded into a resource-theoretic framework that generalizes the standard resource theory of coherence. In particular, POVM-incoherent (free) states and operations were established. In this work, we explore features of this framework which arise due to the rich structure of POVMs compared to projective measurements. Moreover, we introduce a rigorous, probabilisitic framework for POVM-based coherence measures and free operations. This leads to the introduction of new, strongly monotonic resource measures that neatly generalize well-known standard coherence measures. Finally, we show that the relative entropy of POVM-coherence is equal to the cryptographic randomness gain, providing an important operational meaning to the concept of coherence with respect to a general measurement.

I. INTRODUCTION

In quantum technologies, particular properties of quantum states and channels become valuable resources for the application. For example, quantum entanglement enables superior performance in nonlocal games compared to classical resources, which can be utilized for the device-independent distribution of a secret key [1, 2]. Quantum resource theories (QRTs) [3–5] provide a versatile, application-independent methodology for the quantitative analysis of resources. The QRT framework has been applied to different quantum phenomena such as entanglement [6, 7], purity [8], asymmetry [9, 10], thermodynamics [11] and coherence [12–14]. In recent years, the core common structure of QRTs has been identified [15, 16]. In physical setups, the feasible quantum operations are usually constrained, either due to practical limitations or fundamental physical laws such as energy conservation. Consequently, only a subclass of operations can be (easily) realized, which are called free operations. Properties of quantum states that cannot be created by free operations are considered a resource. States without resource content are called free states. Building on these basic notions, it is possible to develop a rigorous quantitative framework which yields insights into the different means of quantifying a resource, the optimal distillation and dilution of the resource and the possibility of interconversion of resource states under the given constraints.

Quantum coherence [14], i.e., the feature of quantum systems to be in a superposition of different states is at the core of quantum mechanics. In particular, coherence underlies quantum entanglement [17] which plays a central role in quantum communication and computing. The resource theory of coherence is formulated with respect to a distinguished basis of a Hilbert space, the incoherent basis $\{|i\rangle\}$, which defines free states as the states that are diagonal in this basis. For instance, in quantum thermodynamics $\{|i\rangle\}$ is the energy eigenbasis and work can be extracted by a thermal process which removes the off-diagonal entries of the state of the system [18]. Equivalently, coherence can be defined with respect to the von Neumann measurement $\mathbf{P} = \{|i\rangle\langle i|\}$ such that free states arise as post-measurement states of $\mathbf{P}$.

However, coherence as an intrinsic property of quantum states should be defined with respect to the most general quantum measurements, namely, positive-operator-valued measures (POVMs). This is because POVMs describe the most general type of quantum observable and can have a real operational advantage compared to any projective measurement, see e.g. [19]. A notion of *coherence with respect to a general measurement* is meaningful if i) it can be embedded in a consistent resource theory ii) POVM-based coherence measures have interesting operational interpretations, i.e, they quantify the advantage of states in a quantum information protocol. Recently, a resource theory of quantum state coherence with respect to an arbitrary POVM was introduced and studied [20]. Here, we develop this framework further by discussing selected features that are distinct from standard coherence theory. In particular, we answer point ii) by providing an important operational interpretation of the most fundamental POVM-coherence measure. Moreover, we introduce further operational restrictions on the class of free operations in conjunction with new useful measures of POVM-coherence. We expect that our findings will help to clarify the role of coherence in all quantum technologies employing nonprojective measurements.

The structure of our work is as follows. In Sec. I B we briefly recapitulate the resource theory of POVM-based coherence [20]. Sec. II discusses a particular one-parameter POVM, which describes how standard coherence turns into POVM-based coherence, highlighting features of minimally coherent states and the measurement map. In Sec. III, we show that the relative entropy of POVM-based coherence quantifies the cryptographic randomness of the measurement outcomes in relation to an eavesdropper who has side information about the measured state. This provides an operational interpretation of the resource theory. Subsequently, in Sec. IV, we define and study free Kraus operators as well as selective free operations. Finally, in Sec. V, we introduce new, strongly monotonic POVM-coherence measures and find relations among them.

* felix.bischof@hhu.de

A. Resource theory of block coherence

The resource theory of POVM-based coherence is derived from the framework of block coherence[1], introduced by Åberg [21]. In the latter resource theory, the Hilbert space $\mathcal{H} = \oplus_i \pi_i$ is partitioned into orthogonal subspaces π_i. If we denote the projector on the i-th subspace by P_i, the set $\mathbf{P} = \{P_i\}$ constitutes a projective measurement on $\mathcal{H}$. Block-incoherent (BI, free) states are defined as states of the form

$$\rho_{\mathrm{BI}} = \Delta[\sigma], \quad \sigma \in \mathcal{S}, \tag{1}$$

$$\Delta[\sigma] = \sum_i P_i \sigma P_i, \tag{2}$$

where $\mathcal{S}$ is the set of quantum states and Δ denotes the block-dephasing operation, which sets all entries except the blocks on the diagonal to zero. In other words, block-incoherent states do not possess "outer" coherence across the subspaces π_i. Note that the convex set of block-incoherent states $\mathcal{I}$ is equal to the set of U(1)-symmetric states in the resource theory of asymmetry with the symmetry group $\{U(\theta) = e^{-i\theta \sum_k k P_k}\}$ [22]. A further ingredient of the resource theory are maximally block-incoherent (MBI) operations Λ_{MBI}. These are channels (i.e., completely positive trace-preserving maps) that preserve the set of block-incoherent states[2], that is, $\Lambda_{\mathrm{MBI}}[\mathcal{I}] \subseteq \mathcal{I}$. Finally, the block-coherence content of states can be quantified by suitable measures [21]. The standard example for a measure is the relative entropy of block coherence, which has the form

$$C_{\mathrm{rel}}(\rho, \mathbf{P}) = S(\Delta[\rho]) - S(\rho), \tag{3}$$

where S denotes the von Neumann entropy $S(\rho) = -\operatorname{tr}(\rho \log_2 \rho)$. The quantity C_{rel} satisfies the following properties which we view as minimal requirements for a block-coherence measure [20]:

(B1) *Faithfulness:* $C(\rho, \mathbf{P}) \geq 0$ with equality iff $\rho = \rho_{\mathrm{BI}}$.

(B2) *Monotonicity:* $C(\Lambda_{\mathrm{MBI}}[\rho], \mathbf{P}) \leq C(\rho, \mathbf{P})$ for any MBI map.

(B3) *Convexity:* $C(\sum_i p_i \rho_i, \mathbf{P}) \leq \sum_i p_i C(\rho_i, \mathbf{P})$ for all states $\{\rho_i\}$, and probabilities $p_i \geq 0$, $\sum_i p_i = 1$.

Note that the concepts explained so far coincide with their counterparts in the standard resource theory of coherence if all P_i have rank one.

B. Resource theory of coherence based on POVMs

A much broader generalization of standard coherence is provided by the POVM-based resource theory of coherence [20]. POVMs describe the most general type of quantum measurement, namely a collection of n positive operators $\mathbf{E} = \{E_i \geq 0\}_{i=1}^n$ that sum to the identity, $\sum_i E_i = \mathbb{1}$. We will also use the corresponding measurement operators, defined as $A_i = U_i \sqrt{E_i}$. Here, $\sqrt{E_i}$ denotes the unique positive square root of E_i and U_i is an arbitrary unitary. Thus, $A_i^\dagger A_i = E_i$ holds.

Let $\mathbf{E}$ be a POVM on a d-dimensional Hilbert space $\mathcal{H}$. The main idea to define POVM-based coherence theory is to link it to the resource theory of block coherence specified by the *Naimark extension* $\mathbf{P}$ of $\mathbf{E}$. The Naimark extension is a projective measurement with the following property: if the POVM is embedded into a subspace of a higher-dimensional Hilbert space $\mathcal{H}'$ of suitable dimension $d' \geq d$, $\mathbf{P}$ extends $\mathbf{E}$ to the whole space. We denote by $\mathcal{E}$ an (isometric) embedding channel, mapping operators on $\mathcal{H}$ to operators on $\mathcal{H}'$. Consequently, it holds that

$$\operatorname{tr}(E_i \rho) = \operatorname{tr}(P_i \mathcal{E}[\rho]), \quad \text{for all } \rho \in \mathcal{S}, \tag{4}$$

that is, $\mathbf{P}$ has the same expectation values for any embedded state $\mathcal{E}[\rho]$ as $\mathbf{E}$ for ρ. Therefore, it is natural to define the coherence of a state ρ w.r.t. a POVM $\mathbf{E}$ as the block coherence of $\mathcal{E}[\rho]$ w.r.t. the Naimark extension $\mathbf{P}$ of $\mathbf{E}$, namely

$$C(\rho, \mathbf{E}) \coloneqq C(\mathcal{E}[\rho], \mathbf{P}), \tag{5}$$

where the function C on the right denotes any unitarily-covariant block-coherence measure [20]. Note that the Naimark extension of a POVM $\mathbf{E}$, in particular its dimension d', is not unique[3]. Therefore, one should ensure that the right side of Eq. (5) does not depend on the choice of Naimark extension $\mathbf{P}$. This property was shown in [20] for the case of $C(\rho', \mathbf{P}) = C_{\mathrm{rel}}(\rho', \mathbf{P})$ from Eq. (3). One obtains the relative entropy of POVM-based coherence

$$C_{\mathrm{rel}}(\rho, \mathbf{E}) = H(\{p_i(\rho)\}) + \sum_i p_i(\rho) S(\rho_i) - S(\rho), \tag{6}$$

with $p_i(\rho) = \operatorname{tr}(E_i \rho)$, $\rho_i = A_i \rho A_i^\dagger / p_i$, $A_i = \sqrt{E_i}$, and the Shannon entropy $H(\{p_i(\rho)\}) = -\sum_i p_i \log_2 p_i$. In the special case of $\mathbf{E}$ being a von Neumann measurement, $E_i = |i\rangle\langle i|$, $C_{\mathrm{rel}}(\rho, \mathbf{E})$ corresponds to the standard relative entropy of coherence. From Def. (5) it follows that for some POVMs the set of states with zero coherence (POVM-incoherent states ρ_{PI}) is empty [20]. The generalization of incoherent states are states with *minimal* coherence $\rho_{\min}$, which form a set $\mathcal{M}$ that has similar properties as the standard incoherent set: it is nonempty, convex, and closed under POVM-incoherent operations, which are defined below.

POVM-incoherent (free) operations can be derived from block-incoherent operations on the enlarged space. Let Λ'_{MBI} be a block-incoherent map on states $\rho' \in \mathcal{S}'$ on the Naimark space with the additional property that the set of embedded states $\{\mathcal{E}[\rho] \in \mathcal{S}' : \rho \in \mathcal{S}\}$ is closed under Λ'_{MBI}. Then, the following channel is called a (maximally) POVM-incoherent operation (MPI) [20]

$$\Lambda_{\mathrm{MPI}}[\rho] = \mathcal{E}^{-1} \circ \Lambda'_{\mathrm{MBI}} \circ \mathcal{E}[\rho]. \tag{7}$$

POVM-coherence measures and MPI maps are the main constituents of the resource theory of quantum state coherence based

[1] In Åberg's work block coherence is called superposition. However, since block coherence is a generalization of coherence with very similar structure, we find this name more suitable from the current literature perspective.

[2] In the resource theory of asymmetry, the free operations usually considered in the literature [9, 10, 23, 24] are the group-covariant operations, i.e., channels that commute with all unitary channels obtained from the symmetry group. In the language of coherence theory, these operations are the translationally-invariant operations [24], which form a strict subset of the maximal set of free operations MBI we consider here [25].

[3] For instance, given any Naimark extension, one can always increase the dimension of each effect by adding projections on additional degrees of freedom.

on POVMs. Crucially, these two concepts are consistent with each other by construction, as any POVM-based coherence measure (5) satisfies:

(P1) *Faithfulness:* $C(\rho,\mathbf{E}) \geq 0$ with equality iff $\rho = \rho_{\text{PI}}$.

(P2) *Monotonicity:* $C(\Lambda_{\text{MPI}}[\rho],\mathbf{E}) \leq C(\rho,\mathbf{E})$ for any MPI map with respect to $\mathbf{E}$.

(P3) *Convexity:* $C(\rho,\mathbf{E})$ is convex in ρ.

See Ref. [20] for a detailed discussion of the concepts. The question whether POVM-coherence measures satisfy *strong* monotonicity is an open problem that will be addressed and answered in Sec IV.

II. MINIMALLY COHERENT STATES AND THE MEASUREMENT MAP

In this section, we examine a one-parameter POVM to illustrate how standard coherence theory turns into POVM-based coherence. Moreover, this example sheds light on two natural questions in the context of the generalized notion of coherence: i) does the maximally mixed state always contain the lowest amount of coherence? ii) is the measurement map $\Lambda_{\mathbf{E}}[\rho] = \sum_i \sqrt{E_i}\rho\sqrt{E_i}$ POVM-incoherent for any POVM? In standard coherence theory, both questions can be answered in the affirmative. However, our example shows that this does not hold in general.

To illustrate the amount of POVM-based coherence in states, we discuss a POVM representing the continuous distortion from a von Neumann measurement into a non-projective POVM. Concretely, we consider $\mathbf{E}(\delta) = \{E_i(\delta)\}_{i=1}^3$ which coincides for $\delta = 0$ with the qubit Y-measurement, and for $\delta = 1$ with the qubit trine POVM, whose measurement directions $\vec{m}_i$ form an equilateral triangle on the xy-plane of the Bloch sphere. With the Bloch representation of qubit POVMs

$$\begin{aligned} E_i &= \alpha_i(\mathbb{1} + \vec{m}_i\cdot\vec{\sigma}) \quad \text{with} \quad \alpha_i \geq 0 \\ \sum_i \alpha_i = 1, &\quad \sum_i \alpha_i\vec{m}_i = 0, \end{aligned} \tag{8}$$

the POVM elements $E_i(\delta)$ are given by the parameters

$$\begin{aligned} \alpha_1 &= \frac{\delta}{3}, \quad \alpha_2 = \alpha_3 = \frac{1}{2}\left(1-\frac{\delta}{3}\right) \\ \vec{m}_1 &= (1,0,0)^T \quad \text{and with} \quad t := \frac{\delta}{3-\delta} \\ \vec{m}_2 &= (-t,\sqrt{1-t^2},0)^T \\ \vec{m}_3 &= (-t,-\sqrt{1-t^2},0)^T. \end{aligned} \tag{9}$$

The effects $E_i(\delta)$ are linearly independent (except for $\delta = 0$) as the measurement directions form a triangle [26]. Moreover, since $|\vec{m}_i| = 1$, the effects have rank one, except for $\delta = 0$ where the first effect has rank zero. Thus, $\mathbf{E}(\delta)$ is an *extremal* POVM for any δ, i.e., it cannot be written as a mixture of two other POVMs, and in this sense does not contain classical noise. In Fig. 1, we plot the POVM-based coherence of selected states, as well as the minimally and maximally achievable coherence for all values of δ. Interestingly, the figure shows that for $0 < \delta < 1$, the state with minimal coherence is distinct from the maximally mixed state. We abstain from stating the explicit form of $\rho_{\min}(\delta)$ in the range $0 < \delta < 1$ as it is too cumbersome. However, we report that in this interval the maximal eigenvalue takes values $0.5 < \|\rho_{\min}(\delta)\|_\infty \lesssim 0.6$.

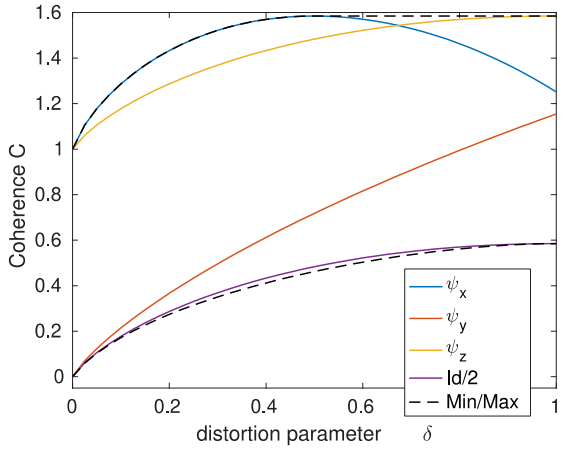

FIG. 1. The relative entropy of POVM-based coherence plotted for selected states with respect to the POVM $\mathbf{E}(\delta)$ defined in Eq. (9) for all values of the distortion parameter δ. The states ψ_x,ψ_y,ψ_z denote the $+1$-eigenstates of the Pauli matrices $\sigma_x,\sigma_y,\sigma_z$, respectively. The lowest solid line corresponds to the maximally mixed state. The dashed lines indicate the achievable minimal and maximal coherence, respectively, which were obtained analytically (by Karush-Kuhn-Tucker conditions [20]).

This property can be utilized to show that the measurement map of the POVM $\mathbf{E}$, defined as

$$\Lambda_{\mathbf{E}}[\rho] = \sum_i \sqrt{E_i}\rho\sqrt{E_i}, \tag{10}$$

which is unital, $\Lambda_{\mathbf{E}}[\mathbb{1}] = \mathbb{1}$, is not incoherent in general. A counterexample is provided by the POVM $\mathbf{E}(\delta)$: Table I shows for selected parameters of δ that $\Lambda_{\mathbf{E}}$ increases the coherence of $\rho_{\min}$ for $0 < \delta < 1$. However, note that $\Lambda_{\mathbf{E}}$ from Eq. (10) is POVM-incoherent for any projective measurement but also for certain nonprojective measurements like the qubit trine POVM [20].

δ	$C_{\text{rel}}(\rho_{\min})$	$C_{\text{rel}}(\Lambda_{\mathbf{E}}[\rho_{\min}])$	$C_{\text{rel}}(\mathbb{1}/2)$
0	0	0	0
0.4	0.412	0.427	0.433
0.5	0.462	0.476	0.483
0.6	0.503	0.514	0.522
1	0.585	0.585	0.585

TABLE I. POVM-based coherence of states w.r.t. $\mathbf{E}(\delta)$ for selected values of δ. For $\delta \in \{0,1\}$, the maximally mixed state $\mathbb{1}/2$ is a state $\rho_{\min}$ of minimal coherence. Moreover, the measurement map $\Lambda_{\mathbf{E}}$ is incoherent in these cases and thus does not increase the coherence of $\rho_{\min}$. For $0 < \delta < 1$, the maximally mixed state $\mathbb{1}/2$ does not have minimal coherence and $\Lambda_{\mathbf{E}}$ increases the coherence of $\rho_{\min}$.

III. POVM-BASED COHERENCE AND PRIVATE RANDOMNESS

In Ref. [20], the relative entropy of POVM-based coherence $C_{\mathrm{rel}}(\rho,\mathbf{E})$ from Eq. (6) was established as a measure of coherence with respect to general measurements. However, in the previous work the operational meaning of this measure was left open. In this section, we show that $C_{\mathrm{rel}}(\rho,\mathbf{E})$ quantifies the private randomness generated by the POVM $\mathbf{E}$ on the state ρ with respect to an eavesdropper holding optimal side information about the measured state. This is a relevant result for quantum randomness generation and cryptography, which generalizes the findings from Refs. [27, 28], where it was shown that the standard relative entropy of coherence corresponds to the quantum randomness of a von Neumann measurement.

We consider a POVM $\mathbf{F} = \{F_i\}$ that is measured on a state ρ_A on a quantum system A, such that the measurement outcomes i are stored in the register X, see Fig. 2. An eavesdropper holds maximal side information about ρ_A, i.e., all degrees of freedom correlated with A in the form of a purifying system E such that $|\psi\rangle_{AE}$ with $\rho_A = \mathrm{tr}_E(|\psi\rangle\langle\psi|_{AE})$ describes the joint pure state. After the measurement $\mathbf{F}$, the joint state is given by

$$\tilde{\rho}_{XAE} = \sum_i p_i |i\rangle\langle i|_X \otimes |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|_{AE}, \tag{11}$$

where $p_i = \mathrm{tr}(F_i\rho_A)$ denotes the probability to obtain outcome i. The pure post-measurement states $|\tilde{\psi}_i\rangle_{AE} = \frac{1}{\sqrt{p_i}}(A_i \otimes \mathbb{1})|\psi\rangle_{AE}$ are defined by the measurement operators A_i that implement the POVM, that is, $F_i = A_i^\dagger A_i$.

Let $S(X|E)_\rho = S(\rho_{XE}) - S(\rho_E)$ denote the conditional von Neumann entropy of X given E on the state ρ. We define the *randomness* contained in the random variable $X = (i, p_i)$ of the measurement outcomes of $\mathbf{F}$ as

$$R_{X|E}(\rho_A) = \min_{|\psi\rangle_{AE}} S(X|E)_{\tilde{\rho}}, \tag{12}$$

where $\tilde{\rho} = \tilde{\rho}_{XE}$ is obtained from Eq. (11) by tracing out A and the minimum is taken over all purifications $|\psi\rangle_{AE}$ of ρ_A. This choice of randomness quantification is relevant in practice, as it describes the asymptotic private randomness, i.e., unpredictability of the measurement outcomes. Indeed, for an eavesdropper employing an independent and identically distributed (IID) attack in an n-round protocol, the single-round von Neumann entropy is related by the quantum asymptotic equipartition property [29] to the smooth quantum min-entropy $H_{\min}^{\varepsilon}(X^n|E^n)$ of all n rounds. The latter quantity has been proven to quantify composable security in quantum randomness generation and cryptography. More precisely, $H_{\min}^{\varepsilon}(X^n|E^n)$ is equal to the minimal number of bits needed to reconstruct X^n from E^n, except with probability of order ε [2, 30].

Proposition 1. Let Eve hold a purification of ρ_A. The private randomness generation rate is equal to the relative entropy of POVM-based coherence, $R_{X|E}(\rho_A) = C_{\mathrm{rel}}(\rho_A,\mathbf{F})$, for any possible POVM $\mathbf{F}$ measured on ρ_A generating the outcome random variable X.

Proof. – First, note that the local measurement $\mathbf{F}$ on A leaves the state $\rho_E = \mathrm{tr}_A(|\psi\rangle\langle\psi|_{AE})$ invariant, i.e., $\tilde{\rho}_E = \rho_E$. Moreover, it holds that $S(\rho_E) = S(\rho_A)$ since $\rho_{AE} = |\psi\rangle\langle\psi|_{AE}$ is pure, and likewise $S(\tilde{\rho}_{A|i}) = S(\tilde{\rho}_{E|i})$ since $\tilde{\rho}_{AE|i} = |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|_{AE}$ is pure. This argument is a direct consequence of the Schmidt decomposition of pure states [31]. Therefore, it holds that

$$\begin{aligned} R_{X|E}(\rho_A) &= \min_{|\psi\rangle_{AE}} \left\{ S\Big(\sum_i p_i|i\rangle\langle i|_X \otimes \tilde{\rho}_{E|i}\Big) - S(\tilde{\rho}_E) \right\} \\ &= \min_{|\psi\rangle_{AE}} \left\{ H(\{p_i\}) + \sum_i p_i S(\tilde{\rho}_{E|i}) - S(\rho_E) \right\} \\ &= H(\{p_i\}) + \sum_i p_i S(\tilde{\rho}_{A|i}) - S(\rho_A). \end{aligned} \tag{13}$$

In the first line, we inserted the state $\tilde{\rho}_{XE}$ from Eq. (11) into Eq. (12). In the second equation, we employed the joint entropy theorem [31]. The minimization can be dropped in the last step, as all quantities are independent of the choice of purification $|\psi\rangle_{AE}$. By inspecting Eq. (6) we see that the expression in the last line is equal to $C_{\mathrm{rel}}(\rho_A,\mathbf{F})$. □

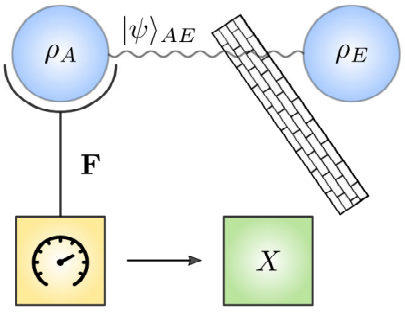

FIG. 2. The relation between private randomness and POVM-based coherence. The eavesdropper Eve has maximal side information about the state ρ_A, namely a purification $|\psi\rangle_{AE}$. Nonetheless, if ρ_A possesses coherence with respect to the POVM $\mathbf{F}$, the measurement outcomes $X = i$ contain secrecy with respect to Eve. That is, the asymptotic randomness generation rate is given by $R_{X|E}(\rho_A) = C_{\mathrm{rel}}(\rho_A,\mathbf{F})$, with the relative entropy of POVM-based coherence defined in Eq. (6).

This result explains why noisy POVMs typically lead to higher values of POVM-based coherence than projective measurements. The noise injects randomness into the outcomes X, which cannot be predicted by an eavesdropper with side information about the measured state. It is crucial that the eavesdropper does not have access to the measurement device, i.e., any noise in the measurement device is trusted. However, if the POVM $\mathbf{E}$ is extremal, the results of Ref. [32–35] show that an eavesdropper cannot get additional knowledge about the measurement outcomes by preprogramming the measurement device. Extremal measurements such as the qubit trine POVM are thought to possess intrinsic quantum noise [26], explaining why even the maximally mixed state can generate nonzero trusted randomness. The POVM $\mathbf{E}(\delta)$ from Eq. (9) is extremal for any $\delta \in [0,1]$. Thus, Fig. 1 shows the generated private randomness $R_{X|E}(\rho)$ for selected states ρ and the advantage of POVMs over projective measurements. In particular, for $\delta \geq \frac{1}{2}$, $\mathbf{E}(\delta)$ yields up to $\log_2(3) \approx 1.58$ private random bits per measurement, compared to maximally one bit for qubit projective measurements.

IV. PROBABILISTICALLY FREE OPERATIONS AND STRONG MONOTONICITY

POVM-incoherent operations as defined in Eq. (7) form the set MPI, that is, the largest class of channels that cannot create POVM-based coherence. Thus, MPI generalizes the set of maximally-incoherent operations MIO [14]. However, in practice it is useful to also have a notion of *selective* POVM-incoherent operations, which we introduce in this section. These operations cannot create coherence, not even probabilistically, when a particular outcome of the channel is selected. This stronger notion of incoherent operations was introduced in Ref. [12] for the standard resource theory of coherence under the name of incoherent operations (IO). It holds that incoherent operations are strictly included in the maximal set, IO $\subset$ MIO.

A. Block-incoherent Kraus operators

As a first building block, we need to introduce Kraus operators that cannot create block coherence. Let $\mathbf{P}$ be any projective measurement defining the Hilbert space partition $\mathcal{H}' = \oplus_i \pi_i$, where $\pi_i = \operatorname{im} P_i$. In Sec. I B we have introduced the block-dephasing operation Δ and block-incoherent states in Eq. (1). Consequently, block-incoherent pure states are element of the set $\{|\varphi_i\rangle\}_i$, where $|\varphi_i\rangle$ denotes any normalized state vector such that

$$|\varphi_i\rangle \in \operatorname{im} P_i. \tag{14}$$

Note that if $\dim P_i \geq 2$, the above set is not finite as superpositions within $\operatorname{im} P_i$ are allowed.

Let $\{K'_l\}$ be a set of Kraus operators on $\mathcal{H}'$, that is, the operators satisfy the normalization condition $\sum_l (K'_l)^\dagger K'_l = \mathbb{1}$. We call a Kraus operator block-incoherent if

$$K'_l|\varphi_i\rangle \propto |\varphi_j\rangle \tag{15}$$

holds for all block-incoherent pure states $|\varphi_i\rangle$. Note that in analogy to the case in standard coherence theory [13] block-incoherent Kraus operators have the form

$$K'_l = \sum_i P_{f(i)} C_l P_i, \tag{16}$$

where f is some index function, which has to be chosen together with the complex matrix C_l on $\mathcal{H}'$ such that normalization holds. We call a Kraus operator K'_l *strictly* block-incoherent, if f is invertible, that is, an index permutation. In this case, also $(K'_l)^\dagger$ is block-incoherent.

B. POVM-incoherent Kraus operators

Next, we construct Kraus operators that cannot create POVM-coherence in analogy to the construction of MPI operations (7). We consider a POVM $\mathbf{E}$ on the d-dimensional space $\mathcal{H}$ and any Naimark extension $\mathbf{P}$ of it, defined on the d'-dimensional space $\mathcal{H}'$. The (Naimark) embedding of $\mathcal{H}$ into $\mathcal{H}'$ is given by $\mathcal{H} \oplus 0 =: \mathcal{H}_\mathcal{E}$, which is a choice we make for the sake of concreteness without loss of generality. Define the operator

$$T = \begin{pmatrix} \mathbb{1} \\ 0 \end{pmatrix}, \tag{17}$$

where 0 denotes the zero matrix of size $(d'-d)\times d$. Consequently, operators X on $\mathcal{H}$ are transformed to Naimark space operators by the isometric channel $\mathcal{E}[X] = TXT^\dagger$. It holds that $T^\dagger T = \mathbb{1}$ and $TT^\dagger = \mathbb{1} \oplus 0 =: \Pi_\mathcal{E}$.

Let $\{K'_l\}$ be a set of block-incoherent Kraus operators (15) on $\mathcal{H}'$, where any operator additionally satisfies

$$K'_l \Pi_\mathcal{E} = \Pi_\mathcal{E} K'_l \Pi_\mathcal{E}. \tag{18}$$

In other words, K'_l maps the embedded original space $\mathcal{H} \oplus 0$ to itself, which we call the subspace-preserving property. It is fulfilled if and only if all Kraus operators are of the form

$$K'_l = \left(\begin{array}{c|c} * & * \\ \hline 0 & * \end{array}\right), \tag{19}$$

where 0 denotes the zero matrix of size $(d' - d) \times d$ and where $*$ represents matrices of suitable dimension.

Definition 1. We call the following operator on $\mathcal{H}$ a POVM-incoherent (PI) Kraus operator:

$$K_l = T^\dagger K'_l T, \tag{20}$$

where T is given in (17) and K'_l satisfies (15), (18) and normalization.

In Eq. (20), the operators $T^\dagger$ and T extract the upper left $d \times d$ block of the $d' \times d'$-matrix K'_l. One can readily check that a PI set $\{K_l\}$ satisfies normalization by construction. At this point, we need to ensure that the above definition is not ambiguous.

Proposition 2. The set containing all POVM-incoherent (PI) Kraus operators K_l does not depend on the choice of Naimark extension used to define it, see Eq. (20).

The proof can be found in the Appendix A. In the special case of a von Neumann measurement, $\mathbf{E}$ can be chosen as its own Naimark extension such that $d' = d$. Thus, in this case Def. 1 and Prop. 2 imply that PI Kraus operators are equivalent to standard incoherent Kraus operators.

C. Selective free operations and strong monotonicity

Building on the previous section, we are ready to define two classes of probabilistically free channels. These have the property that even when we post-select outcomes of the operation, POVM-coherence cannot be created from an incoherent input state. We call a channel Λ a *selective* POVM-incoherent (PI) operation, if it admits a Kraus decomposition $\Lambda[X] = \sum_l K_l X K_l^\dagger$ such that all operators K_l are POVM-incoherent (20). Moreover, we call Λ *strictly* POVM-incoherent (SPI), if additionally all adjoint operators $(K_l)^\dagger$ are POVM-incoherent. These definitions clearly generalize the classes of incoherent operations IO and

strictly incoherent operations SIO [14], respectively. We obtain the following hierarchy of POVM-incoherent operations

$$\text{SPI} \subseteq \text{PI} \subseteq \text{MPI}, \tag{21}$$

where MPI denotes the maximal set of POVM-incoherent operations from Eq. (7).

This leads to the following definition, which extends the requirements on a POVM-coherence measure $C(\rho,\mathbf{E})$ from Sec. I B. It guarantees that free operations cannot create coherence on average when the observer has access to measurement results.

(P2s) *Strong monotonicity of POVM-coherence measure:* $C(\rho,\mathbf{E})$ does not increase on average under selective POVM-incoherent operations PI, i.e.,

$$\sum_l p_l C(\rho_l,\mathbf{E}) \leq C(\rho,\mathbf{E}) \tag{22}$$

for any set of POVM-incoherent Kraus operators K_l defining probabilities $p_l = \mathrm{tr}(K_l\rho K_l^\dagger)$ and post-measurement states $\rho_l = K_l\rho K_l^\dagger/p_l$.

(B2s) *Strong monotonicity of block-coherence measure:* Same as (P2s) for the special case of projective measurements $\mathbf{E} = \mathbf{P}$ and selective block-incoherent operations BI.

Note that as a consequence of convexity, any measure that obeys (P2s) also satisfies (P2) for the class of PI operations, in analogy to e.g. [12]. As in Ref. [20] we can show that POVM-coherence measures, by construction, inherit the properties of the underlying block-coherence measure.

Proposition 3. Let $C(\rho,\mathbf{E})$ be a POVM-based coherence measure derived via (5) from a block-coherence measure $C(\rho',\mathbf{P})$ that obeys strong monotonicity (B2s). Then, $C(\rho,\mathbf{E})$ obeys strong monotonicity (P2s) with respect to PI operations.

Proof. – In the following, we make use of the constructions from Sec. IV B. Let $\{K_l\}$ be a set of POVM-incoherent Kraus operators, leading to the post-measurement states $\rho_l = K_l\rho K_l^\dagger/p_l$. Embedding these yields Naimark space operators given by

$$\begin{aligned} p_l\mathcal{E}[\rho_l] = TK_l\rho K_l^\dagger T^\dagger &= TT^\dagger K_l' T\rho T^\dagger (K_l')^\dagger TT^\dagger \\ &= \Pi_\mathcal{E} K_l'\mathcal{E}[\rho](K_l')^\dagger\Pi_\mathcal{E}, \end{aligned} \tag{23}$$

where we have used $\mathcal{E}[\rho] = T\rho T^\dagger$, Eq. (20) and $\Pi_\mathcal{E} = TT^\dagger$. Since $\mathcal{E}[\rho] = \Pi_\mathcal{E}\mathcal{E}[\rho]\Pi_\mathcal{E}$, we employ Eq. (18) twice to obtain the following simplification:

$$\begin{aligned} \Pi_\mathcal{E} K_l'\mathcal{E}[\rho](K_l')^\dagger\Pi_\mathcal{E} &= \Pi_\mathcal{E} K_l'\Pi_\mathcal{E}\mathcal{E}[\rho]\Pi_\mathcal{E}(K_l')^\dagger\Pi_\mathcal{E} \\ &= K_l'\mathcal{E}[\rho](K_l')^\dagger. \end{aligned} \tag{24}$$

Thus, we have shown that $p_l\mathcal{E}[\rho_l] = K_l'\mathcal{E}[\rho](K_l')^\dagger$, which immediately implies the desired relation:

$$\begin{aligned} \sum_l p_l C(\rho_l,\mathbf{E}) &= \sum_l p_l C(\mathcal{E}[\rho_l],\mathbf{P}) \\ &= \sum_l p_l C(K_l'\mathcal{E}[\rho](K_l')^\dagger/p_l,\mathbf{P}) \\ &\leq C(\mathcal{E}[\rho],\mathbf{P}) = C(\rho,\mathbf{E}). \end{aligned} \tag{25}$$

In the first and last line we have used Eq. (5) and the inequality holds since $C(\rho',\mathbf{P})$ is by assumption strongly monotonic (B2s) with respect to block-incoherent Kraus operators K_l'. □

An example is given by the relative entropy of block coherence $C_{\text{rel}}(\rho',\mathbf{P})$, which satisfies (B2s), as one can prove analogously to Ref. [12] for the standard coherence measure. Thus, Prop. 3 implies that the POVM-coherence measure $C_{\text{rel}}(\rho,\mathbf{E})$ from Eq. (6) is strongly monotonic.

V. MORE MEASURES OF POVM-BASED COHERENCE

So far, the relative-entropy-based quantifier introduced in Ref. [20] is the only known well-defined measure of POVM-based coherence. In this section we introduce further POVM-coherence measures, which are generalizations of standard coherence measures known in the literature [14]. As before, $\mathbf{E}$ is a POVM on $\mathcal{H}$ and $\mathbf{P}$ any Naimark extension of it on the space $\mathcal{H}'$. We denote by $\mathcal{S}$ ($\mathcal{S}'$) the set of density matrices on $\mathcal{H}$ ($\mathcal{H}'$).

First, we discuss distance-based block-coherence quantifiers, which are defined as

$$C(\rho',\mathbf{P}) = \inf_{\sigma\in\mathcal{S}'} D(\rho',\Delta[\sigma]), \tag{26}$$

where $D \geq 0$ is a distance such that $D(\rho,\sigma) = 0 \Leftrightarrow \rho = \sigma$ and Δ is the block-dephasing operation from Eq. (2). The infimum runs over quantum states $\sigma \in \mathcal{S}'$. In Ref. [20] it was shown that a distance-based quantifier satisfies monotonicity (B2) (see I A) if D is contractive under quantum operations, that is, $D(\Lambda[\rho],\Lambda[\sigma]) \leq D(\rho,\sigma)$ holds for any channel Λ.

Distance-based POVM-coherence measures $C(\rho,\mathbf{E})$ are derived from the measures $C(\rho',\mathbf{P})$ (26) via Eq. (5). We show below that this class of measures is independent of the choice of Naimark extension. Importantly, this implies that the POVM-coherence measure coincides for von Neumann measurements with the corresponding standard coherence measure [14].

Observation 1. Let $C(\rho,\mathbf{E})$ be a POVM-based coherence measure that is well-defined, i.e., it is invariant under the choice of Naimark extension $\mathbf{P}$ in Eq. (5). Then, in the special case of orthogonal rank-1 (von Neumann) measurements, $C(\rho,\mathbf{E})$ is equal to its counterpart in standard coherence theory.

Proof. – The assertion holds because for the POVM $E_i = |i\rangle\langle i|$, the Naimark extension can be chosen as $\mathbf{P} = \mathbf{E}$ and the embedding can be chosen trivial, $\mathcal{E}[\rho] = \rho$. Thus, the independence property together with Eq. (5) guarantee that the POVM-based measure generalizes the standard measure. Note that the same argument holds for projective measurements, where $E_i = P_i$. □

Proposition 4. Any distance-based POVM-coherence measure $C(\rho,\mathbf{E})$ defined via Eqs. (5) and (26) is invariant under the choice of Naimark extension if the distance is contractive.

Proof. – Let $\mathbf{P}$, $\hat{\mathbf{P}}$ be two Naimark extensions of the same POVM $\mathbf{E}$ such that $\mathrm{rank}\,\hat{P}_i \leq \mathrm{rank}\,P_i$. The corresponding block-dephasing operations are denoted $\Delta,\hat{\Delta}$. We need to show that $C(\mathcal{E}[\rho],\mathbf{P}) = C(\mathcal{E}[\rho],\hat{\mathbf{P}})$. In the Appendix A we show that there exists a channel (completely positive trace-preserving map) $\mathcal{N}$ which satisfies $\mathcal{N}\circ\mathcal{E} = \mathcal{E}$ and $\mathcal{N}\circ\Delta = \hat{\Delta}\circ\mathcal{N}$ [20].

Let $C(\rho',\mathbf{P}) = D(\rho',\Delta[\sigma^*])$ be a distance-based block coherence measure, where σ^* denotes a state that achieves the minimum. Then, it holds that

$$\begin{aligned} C(\mathcal{E}[\rho],\mathbf{P}) &= D(\mathcal{E}[\rho],\Delta[\sigma^*]) \\ &\geq D(\mathcal{N}\circ\mathcal{E}[\rho],\mathcal{N}\circ\Delta[\sigma^*]) \\ &= D(\mathcal{E}[\rho],\hat{\Delta}\circ\mathcal{N}[\sigma^*]) \\ &= D(\mathcal{E}[\rho],\hat{\Delta}[\hat{\sigma}]) \geq C(\mathcal{E}[\rho],\hat{\mathbf{P}}), \end{aligned} \tag{27}$$

where we have defined $\hat{\sigma} \coloneqq \mathcal{N}[\sigma^*]$. In the first inequality we have used the contractivity of D. The reverse inequality $C(\mathcal{E}[\rho],\mathbf{P}) \leq C(\mathcal{E}[\rho],\hat{\mathbf{P}})$ follows from similar arguments but is more straightforward: the optimal state $\hat{\Delta}[\hat{\sigma}^*]$ on the smaller Naimark space can be embedded in the larger Naimark space and suitably rotated such that it is incoherent with respect to Δ. This is achieved by the channel $\hat{\mathcal{N}} \coloneqq \mathcal{U}^\dagger \circ \mathcal{Q}$ which satisfies $\hat{\mathcal{N}}\circ\mathcal{E} = \mathcal{E}$ and $\hat{\mathcal{N}}\circ\hat{\Delta} = \Delta\circ\hat{\mathcal{N}}$, see App. A. □

Example: Consider the distance measure $D_{\text{geo}}(\rho,\sigma) = 1 - F^2(\rho,\sigma)$, where the fidelity $F(\rho,\sigma) = \operatorname{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$ quantifies how close two quantum states ρ,σ are. We define the *geometric POVM-based coherence* $C_{\text{geo}}(\rho,\mathbf{E})$ via Eqs. (5) and (26) for the distance D_{geo}. The fidelity satisfies $F^2(\Lambda[\rho],\Lambda[\sigma]) \geq F^2(\rho,\sigma)$ for any quantum operation Λ [31], from which follows that $C_{\text{geo}}(\rho,\mathbf{E})$ obeys monotonicity (P2). Observation 1 implies that this measure generalizes the standard geometric coherence [17].

In the following, we introduce and study the robustness of POVM-based coherence which generalizes the measure from [36]. This quantity is derived from the robustness of block coherence, which is equal to the robustness of asymmetry from Ref. [22] for the U(1) symmetry group $\{U(\theta) = e^{-i\theta\sum_k kP_k}\}$. Let $\mathbf{P}$ be a projective measurement and Δ the corresponding dephasing operator (2). We define the robustness of block coherence of a quantum state ρ as

$$C_{\text{rob}}(\rho,\mathbf{P}) = \min_{\tau,\delta\in\mathcal{S}}\Big\{s\geq 0 : \frac{\rho+s\tau}{1+s} = \Delta[\delta]\Big\} \tag{28}$$

$$= \min_{\delta\in\mathcal{S}}\big\{s\geq 0 : \rho \leq (1+s)\Delta[\delta]\big\}. \tag{29}$$

In other words, $C_{\text{rob}}(\rho,\mathbf{P})$ is the minimal mixing weight s required to make ρ block-incoherent. It is clear that the measure satisfies faithfulness (B1). Moreover, the arguments from Ref. [22] imply that $C_{\text{rob}}(\rho,\mathbf{P})$ satisfies convexity (B3), and strong monotonicity (B2s) under selective block-incoherent operations. Interestingly, the robustness measure can be related to the *maximum relative entropy of block coherence*, which we define as $C_{\max}(\rho,\mathbf{P}) = \min_{\delta\in\mathcal{S}}\{\lambda\geq 0 : \rho\leq 2^\lambda\Delta[\delta]\}$ [37]. By comparison with Eq. (29) we infer that $C_{\max}(\rho,\mathbf{P}) = \log_2[1 + C_{\text{rob}}(\rho,\mathbf{E})]$. A further characterization of C_{rob} is given in the Appendix B.

Now, let $\mathbf{E}$ be a POVM and $\mathbf{P}$ any Naimark extension of it. We employ the standard construction from Eq. (5) to define the *robustness of POVM-based coherence* as

$$C_{\text{rob}}(\rho,\mathbf{E}) \coloneqq C_{\text{rob}}(\mathcal{E}[\rho],\mathbf{P}). \tag{30}$$

The following result establishes $C_{\text{rob}}(\rho,\mathbf{E})$ as a proper measure of POVM-coherence.

Proposition 5. The robustness of POVM-based coherence $C_{\text{rob}}(\rho,\mathbf{E})$ is well-defined and a POVM-coherence measure that satisfies strong monotonicity (P2s). It admits the following form:

$$C_{\text{rob}}(\rho,\mathbf{E}) = \min_{\tau\in\mathcal{S}'}\big\{s\geq 0 : s\tau_{i,j} = -A_i\rho A_j^\dagger \;\forall i\neq j\big\}, \tag{31}$$

where $\tau = \sum_{i,j}\tau_{i,j}\otimes|i\rangle\langle j|$ and $A_i = \sqrt{E_i}$.

Observation 1 implies that in the special case of von Neumann measurements $\mathbf{E} = \{|i\rangle\langle i|\}$, $C_{\text{rob}}(\rho,\mathbf{E})$ coincides with the standard robustness of coherence [36]. The evaluation of C_{rob} in Eq. (31) is a semidefinite program (SDP). It can be simplified to the following form suited for numerical computation, for example, via the open-source MATLAB-based toolbox YALMIP [38]:

$$\begin{aligned} &C_{\text{rob}}(\rho,\mathbf{E}) = \min\sum_i \operatorname{tr}(\sigma_{i,i}) \\ &\text{s.t.}\quad \sigma_{i\neq j,j} = -A_i\rho A_j^\dagger, \quad \sum_{i,j}\sigma_{i,j}\otimes|i\rangle\langle j| \geq 0. \end{aligned} \tag{32}$$

This form is obtained from Prop. 5 by setting $\sigma = s\tau$.

Proof of Prop. 5. – First, we prove that the definition of $C_{\text{rob}}(\rho,\mathbf{E})$ is not ambiguous as it leads to the same quantity for any Naimark extension $\mathbf{P}$ of $\mathbf{E}$. Let $\mathbf{P}$, $\hat{\mathbf{P}}$ be two Naimark extensions of the same POVM $\mathbf{E}$ such that $\operatorname{rank}\hat{P}_i \leq \operatorname{rank}P_i$. The corresponding block-dephasing operations are denoted $\hat{\Delta},\Delta$. It is clear that $C_{\text{rob}}(\mathcal{E}[\rho],\mathbf{P}) \leq C_{\text{rob}}(\mathcal{E}[\rho],\hat{\mathbf{P}})$ since the optimal state $\hat{\Delta}[\hat{\delta}^*]$ in Eq. (29) on the smaller Naimark space can be embedded in the larger Naimark space and suitably rotated such that it is incoherent with respect to Δ. We proceed to prove the reverse inequality by employing the channel $\mathcal{N}$ from the proof of Prop. 4. Take Eq. (29) with optimal quantities s^*,δ^* and apply $\mathcal{N}$ to both sides of the constraint

$$\begin{aligned} \mathcal{E}[\rho] \leq (1+s^*)\Delta[\delta^*] &\Rightarrow \mathcal{N}\circ\mathcal{E}[\rho] \leq (1+s^*)\mathcal{N}\circ\Delta[\delta^*] \\ &\Leftrightarrow \quad \mathcal{E}[\rho] \leq (1+s^*)\hat{\Delta}[\hat{\delta}], \end{aligned} \tag{33}$$

where we have defined $\hat{\delta} = \mathcal{N}[\delta^*]$. Thus, $C_{\text{rob}}(\mathcal{E}[\rho],\hat{\mathbf{P}}) \leq s^* = C_{\text{rob}}(\mathcal{E}[\rho],\mathbf{P})$. Altogether, we conclude that $C_{\text{rob}}(\rho,\mathbf{E})$ is independent of the Naimark extension choice. Moreover, C_{rob} satisfies strong monotonicity (P2s) because of Prop. 3 and Property 2 in Ref. [22].

In order to prove Eq. (31), we use the following result established as Prop. 4 in Ref. [20]. Any POVM-coherence measure can be written as

$$C(\rho,\mathbf{E}) = C(\mathcal{E}_V[\rho],\{\mathbb{1}\otimes|i\rangle\langle i|\}), \tag{34}$$

with the embedding $\mathcal{E}_V[\rho] = V\rho\otimes|1\rangle\langle 1|V^\dagger = \sum_{i,j}A_i\rho A_j^\dagger\otimes|i\rangle\langle j|$ containing an interaction isometry V, and the Naimark extension $\{\mathbb{1}\otimes|i\rangle\langle i|\}$. By using that in this formulation, $\delta\in\mathcal{I} \Leftrightarrow \delta = \sum_i\delta_i\otimes|i\rangle\langle i|$ and employing the parameterization $\tau = \sum_{i,j}\tau_{i,j}\otimes|i\rangle\langle j|$, we obtain

$$\begin{aligned} &C_{\text{rob}}(\rho,\mathbf{E}) \\ &= \min_{\tau,\delta\in\mathcal{S}'}\Big\{s\geq 0 : \sum_{i,j}(A_i\rho A_j^\dagger + s\tau_{i,j})\otimes|i\rangle\langle j| = (1+s)\sum_i\delta_i\otimes|i\rangle\langle i|\Big\} \\ &= \min_{\tau\in\mathcal{S}'}\big\{s\geq 0 : s\tau_{i,j} = -A_i\rho A_j^\dagger \;\forall i\neq j\big\}, \end{aligned} \tag{35}$$

Note that the constraint for $i = j$ was neglected in the last line, since for any s and state τ satisfying the last line, we can define $\delta_i = (A_i\rho A_i^\dagger + s\tau_{i,i})/(1+s)$, which directly implies that $\delta \geq 0$ and $\operatorname{tr}\delta = 1$. □

We also define the following quantifier, the *ℓ_1-norm of POVM-based coherence*: $C_{\ell_1}(\rho,\mathbf{E}) = \sum_{i\neq j}\|P_i\mathcal{E}[\rho]P_j\|_1$, where $\|X\|_1 = \operatorname{tr}(\sqrt{X^\dagger X})$ denotes the trace norm. By making use of Eq. (34) and that $\|X\otimes Y\|_1 = \|X\|_1\|Y\|_1$ holds for operators X,Y, it is straightforward to show that a simplified, local expression holds

$$C_{\ell_1}(\rho,\mathbf{E}) = \sum_{i\neq j}\|A_i\rho A_j^\dagger\|_1. \tag{36}$$

This generalized coherence quantifier satisfies faithfulness (P1), see Prop. 5 in [20], and convexity (P3). Since for a von Neumann measurement $C_{\ell_1}(\rho,\mathbf{E})$ reduces to the standard ℓ_1-norm of coherence, we can infer that the measure does not satisfy monotonicity (P2) for the class MPI in general, see Ref. [39]. However, C_{ℓ_1} satisfies (P2) under MPI for any two-outcome POVM $\mathbf{E} = \{E_i\}_{i=1}^2$, which follows from Proposition 9 of Ref. [21] together with Prop. 3. We leave open for future work whether $C_{\ell_1}(\rho,\mathbf{E})$ satisfies strong monotonicity (P2s) under PI, which holds for von Neumann measurements [12].

For completeness, we show that $C_{\ell_1}(\rho,\mathbf{E})$ is invariant under the choice of Naimark extension and unambigiously given by Eq. (36). Given two Naimark extensions $\mathbf{P}$, $\hat{\mathbf{P}}$, we utilize the isometry Q from App. A satisfying $P_iQ = Q\hat{P}_i$. Further, we employ the unitary U on the larger Naimark space with properties $UP_i = P_iU$ and $U\Pi_\mathcal{E} = Q\Pi_\mathcal{E}$, where $\Pi_\mathcal{E}$ is the projector onto the embedded original space $\mathcal{H}_\mathcal{E}$. Since the trace norm is invariant under multiplication by isometries V,W, $\|X\|_1 = \|VXW^\dagger\|_1$, we have

$$\begin{aligned}\|\hat{P}_i\mathcal{E}[\rho]\hat{P}_j\|_1 &= \|U^\dagger Q\hat{P}_i\mathcal{E}[\rho]\hat{P}_jQ^\dagger U\|_1\\ &= \|P_iU^\dagger Q\mathcal{E}[\rho]Q^\dagger UP_j\|_1 = \|P_i\mathcal{E}[\rho]P_j\|_1.\end{aligned}$$ □

Note that in the special case of rank-one effects E_i, $C_{\mathrm{rel}}(\rho,\mathbf{E})$ and $C_{\ell_1}(\rho,\mathbf{E})$ coincide with the generalized coherence quantifiers proposed in [41].

The following result establishes general relations between POVM-coherence measures that are visualized in Fig. 3. These findings generalize results from Ref. [40].

Proposition 6. Given an n-outcome POVM $\mathbf{E}$, the following inequalities hold for the measures from Eqs. (6), (31), (36):

$$C_{\mathrm{rob}}(\rho,\mathbf{E}) \leq C_{\ell_1}(\rho,\mathbf{E}) \leq n-1, \tag{37}$$

$$C_{\mathrm{rel}}(\rho,\mathbf{E}) \leq \log_2[1 + C_{\mathrm{rob}}(\rho,\mathbf{E})]. \tag{38}$$

Moreover, $C_{\mathrm{rob}}(\psi,\mathbf{E}) = C_{\ell_1}(\psi,\mathbf{E})$ holds for any pure state ψ.

Proof. – First, we prove $C_{\mathrm{rob}}(\rho,\mathbf{E}) \leq n-1$ by showing that $C_{\mathrm{rob}}(\rho',\mathbf{P}) \leq n-1$ for any n-outcome projective measurement $\mathbf{P}$ and any state $\rho' \in \mathcal{S}'$. For that, define $K_{i,j} = (P_i - P_j)/\sqrt{2}$ and consider the expression

$$\begin{aligned}\sum_{i,j}K_{i,j}\rho K_{i,j}^\dagger &= \frac{1}{2}\sum_{i,j}(P_i-P_j)\rho(P_i-P_j)\\ &= \sum_{i,j}P_i\rho P_i - \sum_{i,j}P_i\rho P_j\\ &= n\sum_i P_i\rho P_i - \sum_{i,j}P_i\rho P_j = (n\Delta - \mathrm{id})[\rho].\end{aligned} \tag{39}$$

Consequently, the map $(n\Delta - \mathrm{id})$ admits a Kraus decomposition and is thus completely positive. This implies that $n\Delta[\rho'] - \rho' \geq 0$ holds for any quantum state ρ'. Hence, we obtained $\rho' \leq n\Delta[\rho']$ and by comparison with Eq. (29) we conclude that $C_{\mathrm{rob}}(\rho',\mathbf{P}) = s \leq n-1$.

The relation $C_{\ell_1}(\rho,\mathbf{E}) \leq n-1$ can be shown by evaluating the underlying block-coherence measure for a maximally coherent state. The latter is given by $|\Psi_\mathrm{m}\rangle = \frac{1}{\sqrt{n}}\sum_i|\varphi_i\rangle$ with pure block-incoherent states $|\varphi_i\rangle$ defined in Eq. (14). This leads to

$$\begin{aligned}C_{\ell_1}(|\Psi_\mathrm{m}\rangle,\mathbf{P}) &= \frac{1}{n}\sum_{i\neq j}\|\sum_{k,l}P_i|\varphi_k\rangle\langle\varphi_l|P_j\|_1 = \frac{1}{n}\sum_{i\neq j}\|\,|\varphi_i\rangle\langle\varphi_j|\,\|_1\\ &= \frac{1}{n}\sum_{i\neq j}1 = \frac{1}{n}n(n-1) = n-1.\end{aligned} \tag{40}$$

In the Appendix B we show a further SDP characterization of the robustness of POVM-based coherence. Moreover, this form is used to show that $C_{\mathrm{rob}}(\psi,\mathbf{E}) = C_{\ell_1}(\psi,\mathbf{E})$ for pure states and $C_{\mathrm{rob}}(\rho,\mathbf{E}) \leq C_{\ell_1}(\rho,\mathbf{E})$ in general.

Finally, we show Eq. (38) similar to Ref. [40]. Let s^*,δ^* be the the optimal quantities for $C_{\mathrm{rob}}(\rho,\mathbf{E}) = C_{\mathrm{rob}}(\mathcal{E}[\rho],\mathbf{P})$ in Eq. (29). Using the abbreviation $\rho_\mathcal{E} = \mathcal{E}[\rho]$, it holds that $C_{\mathrm{rel}}(\rho_\mathcal{E},\mathbf{P}) = S(\rho_\mathcal{E}\|\Delta[\rho_\mathcal{E}]) \leq S(\rho_\mathcal{E}\|\Delta[\delta^*])$. Moreover

$$\begin{aligned}&S(\rho_\mathcal{E}\|\Delta[\delta^*])\\ &= \operatorname{tr}\Big[\rho_\mathcal{E}\big(\log_2\rho_\mathcal{E} - \log_2\frac{(1+s^*)\Delta[\delta^*]}{(1+s^*)}\big)\Big]\\ &= \log_2(1+s^*) + \operatorname{tr}[\rho_\mathcal{E}(\log_2\rho_\mathcal{E} - \log_2(1+s^*)\Delta[\delta^*])],\end{aligned} \tag{41}$$

where we have used the definition of the relative entropy $S(\rho\|\sigma) = \operatorname{tr}[\rho(\log_2\rho - \log_2\sigma)]$. On the other hand, Eq. (29) implies that $\rho_\mathcal{E} \leq (1+s^*)\Delta[\delta^*]$. The latter relation together with the fact that the logarithm is operator-monotone yields that the second term in (41) (last line) is non-positive. We conclude that $C_{\mathrm{rel}}(\rho,\mathbf{E}) \leq S(\rho_\mathcal{E}\|\Delta[\delta^*]) \leq \log_2(1+s^*)$ implying the desired relation. □

VI. CONCLUSION AND OUTLOOK

We presented several results on the resource-theoretical concept of coherence with respect to a general quantum measurement. We expect these advances to clarify the role of quantum coherence in information technologies employing nonprojective measurements. In particular, we discussed selected features of POVM-based coherence theory that are distinct from the standard resource theory of coherence. Moreover, we established a probabilistic framework of free transformations in conjunction with resource measures. This led to the introduction of new, strongly monotonic POVM-based coherence measures that generalize well-known coherence measures. We also established relations among the new measures. Finally, we showed that the relative-entropy-based resource measure is equal to the cryptographic randomness gain, providing an important operational meaning to the concept of coherence with respect to a measurement.

Together with Ref. [20], we have paved the way for a detailed operational analysis of POVM-based coherence as a resource,

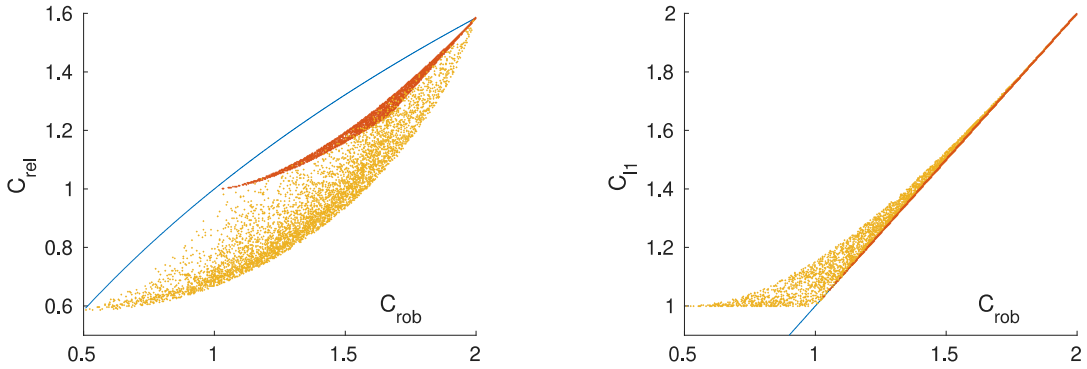

FIG. 3. POVM-coherence measures in relation to the generalized robustness of coherence $s := C_{\mathrm{rob}}(\rho, \mathbf{E})$ for the qubit trine POVM $\mathbf{E}(\delta = 1)$ (9). *Left:* the blue line indicates the bound $C_{\mathrm{rel}}(\rho, \mathbf{E}) \leq \log_2(1 + s)$ from Eq. (38). Red (yellow) dots represent randomly sampled pure (mixed) states. Similar to standard coherence theory [40], the upper bound is not tight. *Right:* the blue, straight line indicates the graph of $C_{\ell_1}(\rho, \mathbf{E}) = s$, on which all pure states lie (red dots). The yellow dots represent mixed states for which $C_{\ell_1}(\rho, \mathbf{E}) \geq s$ holds (37).

akin to what has been achieved in the standard resource theory of coherence [13, 42–44]. The operational analysis includes the investigation of resource distillation and dilution in the asymptotic and single-shot regime, see [45–47]. In particular, it is open whether our theory is reversible, or there are bound resources for a given class of POVM-incoherent operations [48, 49]. An important step towards this goal would consist in a possible simplification of our constructions, e.g., of the MPI and PI operations. Moreover, we expect that virtually all known coherence measures and incoherent channel classes [14] can be generalized to POVMs. It is likely that more operational interpretations of POVM-based coherence measures can be found which link the resource theory to interesting applications in quantum information science. Finally, future work should address the connection of POVM-based coherence with other notions of nonclassicality such as entanglement and purity [17, 50].

ACKNOWLEDGMENTS

We acknowledge financial support from the German Federal Ministry of Education and Research (BMBF). F.B. gratefully acknowledges support from Evangelisches Studienwerk Villigst and from Strategischer Forschungsfonds of the Heinrich Heine University Düsseldorf.

APPENDIX

Appendix A: Relating Naimark extensions of a POVM

In the Supplemental Material of Ref. [20] several relations between Naimark extensions of a POVM were established. In this section, we provide an overview of these results which are used to show that the constituents of our POVM-based coherence theory do not depend on the choice of Naimark extension. In particular, we prove Prop. 2 at the end of this section.

Let $\mathbf{P}$, $\hat{\mathbf{P}}$ be two Naimark extensions of the same n-outcome POVM $\mathbf{E}$ such that $\operatorname{rank} \hat{P}_i \leq \operatorname{rank} P_i$. There exists an isometry $Q : \hat{\mathcal{H}} \to \mathcal{H}'$ from the smaller Naimark spacer to the larger Naimark space such that

$$P_i Q = Q \hat{P}_i \quad \text{and} \tag{A1}$$
$$\mathcal{Q} \circ \hat{\Delta} = \Delta \circ \mathcal{Q}, \tag{A2}$$

where we have defined the isometric channel $\mathcal{Q}[X] = QXQ^\dagger$ and $\hat{\Delta}[X] = \sum_i \hat{P}_i X \hat{P}_i$ denotes the block-dephasing operator.

Moreover, it was shown that there exists a unitary U on the larger Naimark space such that [20]

$$Q\Pi_\mathcal{E} = U\Pi_\mathcal{E} \quad \text{and} \tag{A3}$$
$$\mathcal{Q} \circ \mathcal{E} = \mathcal{U} \circ \mathcal{E}, \tag{A4}$$

where $\mathcal{E}[X] = TXT^\dagger = X \oplus 0$ denotes the embedding operation, see Sec. I B. This unitary can be chosen to be block-diagonal such that it commutes with the Naimark extension effects

$$UP_i = P_i U \quad \text{and} \tag{A5}$$
$$\Delta \circ \mathcal{U} = \mathcal{U} \circ \Delta. \tag{A6}$$

The channel $\mathcal{Q}^\dagger[\rho] = Q^\dagger \rho Q$ is completely positive but not trace-preserving in general. Define the projector $S := QQ^\dagger$ and its complement $S^\perp = \mathbb{1} - S$ for which holds that $S^\perp Q = 0$. We define the completely positive map

$$\mathcal{T}[\rho] := \operatorname{tr}(S^\perp \rho)\mathbb{1}/d_{\min}, \tag{A7}$$

which has Kraus operators

$$L_{\hat{a},b} = \frac{1}{\sqrt{d_{\min}}} |\hat{a}\rangle\langle b| S^\perp, \tag{A8}$$

where $\{|\hat{a}\rangle\}$ ($\{|b\rangle\}$) denotes an orthonormal basis of the smaller (larger) Naimark space. We choose as output basis $|\hat{a}\rangle \in \hat{\mathcal{H}}$ an incoherent basis with respect to $\hat{P}_i$. Consequently, $L_{\hat{a},b}$ cannot create coherence for any input. Define the operators

$$R_m = \begin{cases} Q^\dagger & \text{for } m = 0 \\ L_{\hat{a},b} & \text{for } m \geq 1, \end{cases} \tag{A9}$$

where the index m for $m \geq 1$ runs over all combinations of $(\hat{a}, b)$. The set $\{R_m\}$ is a set of Kraus operators for the channel

$$\mathcal{R} = \mathcal{Q}^\dagger + \mathcal{T}. \tag{A10}$$

It holds that $\mathcal{R} \circ \mathcal{Q} = \mathrm{id}$, i.e., $\mathcal{R}$ is a reversal channel of the isometric channel $\mathcal{Q}$. One can show that the following equation holds [20]

$$\hat{\Delta} \circ \mathcal{R} = \mathcal{R} \circ \Delta. \tag{A11}$$

In addition, it holds that $\mathcal{T} \circ \mathcal{E}[\rho] = \mathrm{tr}(S^\perp \mathcal{E}[\rho])\mathbb{1}/d_{\min} = 0$ and therefore

$$\mathcal{R} \circ \mathcal{E} = \mathcal{Q}^\dagger \circ \mathcal{E}. \tag{A12}$$

Finally, we define the following channel from operators on the larger Naimark space to operators on the smaller Naimark space:

$$\mathcal{N} \coloneqq \mathcal{R} \circ \mathcal{U}, \quad \text{which satisfies} \tag{A13}$$

$$\mathcal{N} \circ \mathcal{E} = \mathcal{E} \quad \text{and} \quad \mathcal{N} \circ \Delta = \hat{\Delta} \circ \mathcal{N}. \tag{A14}$$

The first equality follows from $\mathcal{N} \circ \mathcal{E} = \mathcal{R} \circ \mathcal{U} \circ \mathcal{E} = \mathcal{R} \circ \mathcal{Q} \circ \mathcal{E} = \mathcal{E}$. The second equality follows from $\mathcal{N} \circ \Delta = \mathcal{R} \circ \mathcal{U} \circ \Delta = \hat{\Delta} \circ \mathcal{R} \circ \mathcal{U} = \hat{\Delta} \circ \mathcal{N}$.

Proof of Proposition 2

Proposition 2. The set containing all POVM-incoherent (PI) Kraus operators K_l does not depend on the choice of Naimark extension used to define it, see Eq. (20).

Proof. – Let $\mathbf{P}, \hat{\mathbf{P}}$ be two Naimark extensions of the same POVM $\mathbf{E}$ such that $\mathrm{rank}\, \hat{P}_i \leq \mathrm{rank}\, P_i$. Let $\{K_l = T^\dagger K_l' T\}$ be the set of POVM-incoherent Kraus operators defined via incoherent operators $\{K_l'\}$ of the "larger" Naimark extension $\mathbf{P}$, see Eq. (20). Consider the MBI channel $\Gamma[\rho'] = \sum_l K_l' \rho' (K_l')^\dagger$ on the larger Naimark space. The channel $\hat{\Gamma} \coloneqq \mathcal{R} \circ \mathcal{U} \circ \Gamma \circ \mathcal{U}^\dagger \circ \mathcal{Q}$ is a MBI channel on the smaller Naimark space, that leads to the same (local) MPI operation Λ_{MPI} [20]. We consider the following Kraus decomposition of the channel:

$$\begin{aligned} \hat{\Gamma}[\hat{\rho}] &= \sum_{m,l} R_m U K_l' U^\dagger Q \hat{\rho} Q^\dagger U (K_l')^\dagger U^\dagger R_m^\dagger \\ &= \sum_{m,l} \hat{K}_{m,l} \hat{\rho} \hat{K}_{m,l}^\dagger, \\ \hat{K}_{m,l} &\coloneqq R_m U K_l' U^\dagger Q, \end{aligned} \tag{A15}$$

where R_m was defined in Eq. (A9).

We proceed to show that the set $\{\hat{K}_{m,l}\}$

i) satisfies $\sum_{m,l} \hat{K}_{m,l}^\dagger \hat{K}_{m,l} = \mathbb{1}$,

ii) has the property that each element is incoherent w.r.t. $\hat{\mathbf{P}}$,

iii) leads to the previous set of PI Kraus operators, more precisely, $T^\dagger \hat{K}_{m,l} T = \delta_{m,0} K_l$.

The first claim holds since $\{\hat{K}_{m,l}\}$ is a set of Kraus operators of $\hat{\Gamma}$, which is a completely positive trace-preserving map [20].

For the second claim, consider a block-incoherent pure state $|\varphi_i\rangle = \hat{P}_i |\varphi_i\rangle$, for which holds:

$$\begin{aligned} \hat{K}_{m,l}|\varphi_i\rangle &= \hat{K}_{m,l}\hat{P}_i|\varphi_i\rangle \\ &= R_m U K_l' P_i U^\dagger Q |\varphi_i\rangle \\ &= R_m U P_{f(i)} K_l' P_i U^\dagger Q |\varphi_i\rangle \\ &= R_m P_{f(i)} U K_l' P_i U^\dagger Q |\varphi_i\rangle \\ &= \begin{cases} \hat{P}_{f(i)} Q^\dagger U K_l' P_i U^\dagger Q |\varphi_i\rangle & \text{for } m = 0 \\ L_{\hat{a},b} P_{j(i)} U K_l' P_i U^\dagger Q |\varphi_i\rangle & \text{else.} \end{cases} \end{aligned} \tag{A16}$$

The second equation makes use of (A1) and (A5). In the third line we have used that for an incoherent input, the output of K_l' is incoherent (16). Finally, the last equation follows from the definition of R_m (A9). Note that in any case, the output of the Kraus operator in (A16) is incoherent, see (A8).

For the third claim, we evaluate:

$$\begin{aligned} T^\dagger \hat{K}_{m,l} T &= T^\dagger R_m U K_l' U^\dagger Q T \\ &= T^\dagger R_m U K_l' T \\ &= T^\dagger R_m U \Pi_\mathcal{E} K_l' T \\ &= T^\dagger R_m Q \Pi_\mathcal{E} K_l' T \\ &= \delta_{m,0} T^\dagger K_l' T = \delta_{m,0} K_l. \end{aligned} \tag{A17}$$

In the first line, the definition of $\hat{K}_{m,l}$ (A15) was inserted. The second and fourth line utilize the relations $UT = QT$ and $\Pi_\mathcal{E} = TT^\dagger$. In the third line, we have used that K_l' is subspace-preserving (18). Finally, for the last line, note that according to (A9), $R_0 Q = Q^\dagger Q = \mathbb{1}$, and $R_m Q = 0$ for $m \geq 1$. □

Appendix B: Alternative SDP for generalized robustness measure

In Ref. [22] it was shown that the robustness of block-coherence (asymmetry) can be expressed by the following SDP:

$$\begin{aligned} &C_{\mathrm{rob}}(\rho, \mathbf{P}) = \max \mathrm{tr}(X\rho) - 1, \\ &\text{s.t.} \quad X \geq 0, \quad \Delta[X] = \mathbb{1}. \end{aligned} \tag{B1}$$

where $\Delta[X] = \sum_i P_i X P_i$ denotes the block-dephasing operation. Consider the POVM-coherence measure $C_{\mathrm{rob}}(\rho, \mathbf{E}) = C_{\mathrm{rob}}(\mathcal{E}_V[\rho], \mathbf{P})$, where $P_i = \mathbb{1} \otimes |i\rangle\langle i|$ and $\mathcal{E}_V[\rho] = \sum_{i,j} A_i \rho A_j^\dagger \otimes |i\rangle\langle j|$, see Eq. (34). If we write $X = \sum_{i,j} X_{i,j} \otimes |i\rangle\langle j|$, we directly obtain the SDP:

$$\begin{aligned} &C_{\mathrm{rob}}(\rho, \mathbf{E}) = \max \mathrm{tr}\Big(\sum_{i,j} X_{j,i} A_i \rho A_j^\dagger\Big) - 1 \\ &\text{s.t.} \quad \sum_{i,j} X_{i,j} \otimes |i\rangle\langle j| \geq 0, \quad X_{i,i} = \mathbb{1}. \end{aligned} \tag{B2}$$

Employing this form, we are able to show that $C_{\mathrm{rob}}(\rho, \mathbf{E}) \leq$

$C_{\ell_1}(\rho,\mathbf{E})$ as follows:

$$\begin{aligned} C_{\mathrm{rob}}(\rho,\mathbf{E}) &= \max_{X\geq 0, X_{i,i}=\mathbb{1}} \sum_{i,j} \mathrm{tr}(X_{j,i}A_i\rho A_j^\dagger) - 1 \\ &= \max_{X\geq 0, X_{i,i}=\mathbb{1}} \sum_{i\neq j} \mathrm{tr}(X_{j,i}A_i\rho A_j^\dagger) \\ &= \max_{X\geq 0, X_{i,i}=\mathbb{1}} 2\sum_{i<j} \mathrm{Re}\,\mathrm{tr}(X_{j,i}A_i\rho A_j^\dagger) \\ &\leq \max_{X\geq 0, X_{i,i}=\mathbb{1}} 2\sum_{i<j} |\mathrm{tr}(X_{j,i}A_i\rho A_j^\dagger)| \\ &\leq 2\sum_{i<j} \max_{\|X_{i,j}\|_\infty\leq 1} |\mathrm{tr}(X_{j,i}A_i\rho A_j^\dagger)| \\ &= 2\sum_{i<j} ||A_i\rho A_j^\dagger||_1 = C_{\ell_1}(\rho,\mathbf{E}). \end{aligned} \tag{B3}$$

For the second inequality, we have used that $X \geq 0, X_{i,i} = 1$ implies $\|X_{i,j}\|_\infty \leq \mathbb{1}$, where $||X||_\infty$ denotes the largest singular value of X. Then, we employed the variational characterization of the trace norm, $||R||_1 = \max_{||L||_\infty\leq 1}|\mathrm{tr}(L^\dagger R)|$, which follows from the duality property of the Schatten norms [51].

We proceed that show that $C_{\mathrm{rob}}(\psi,\mathbf{E}) = C_{\ell_1}(\psi,\mathbf{E})$ holds for any pure state $\psi := |\psi\rangle\langle\psi|$. For indices i, j, consider the rank one operator $A_i|\psi\rangle\langle\psi|A_j^\dagger = \sqrt{p_i p_j}|\phi_i\rangle\langle\phi_j|$ with $p_i := \langle\psi|A_i^\dagger A_i|\psi\rangle \leq 1$. The vectors $|\phi_i\rangle = \frac{1}{\sqrt{p_i}}A_i|\psi\rangle$ are normalized and not necessarily orthogonal. Evaluating $C_{\ell_1}(\psi,\mathbf{E})$ yields

$$\begin{aligned} C_{\ell_1}(\psi,\mathbf{E}) &= \sum_{i\neq j} \|A_i|\psi\rangle\langle\psi|A_j^\dagger\|_1 \\ &= \sum_{i\neq j} \sqrt{p_i p_j}\,\||\phi_i\rangle\langle\phi_j|\|_1 \\ &= \sum_{i\neq j} \sqrt{p_i p_j}. \end{aligned} \tag{B4}$$

We define the hermitian operator $\tilde{X} = \sum_{i,j} \tilde{X}_{i,j} \otimes |i\rangle\langle j|$ as

$$\tilde{X} = \sum_{i,j} |\phi_i\rangle\langle\phi_j| \otimes |i\rangle\langle j| + \sum_i (\mathbb{1} - |\phi_i\rangle\langle\phi_i|) \otimes |i\rangle\langle i|. \tag{B5}$$

It holds that $\tilde{X} \geq 0$ since the first term can be written as $|\Omega\rangle\langle\Omega| \geq 0$ with $|\Omega\rangle = \sum_i |\phi_i\rangle \otimes |i\rangle$, while the second term is in spectral decomposition form and apparently positive semidefinite. Moreover, the diagonal blocks of $\tilde{X}$ are equal to the identity, $\tilde{X}_{i,i} = \mathbb{1}$. Thus, $\tilde{X}$ is element of the feasible set of operators X used to obtain $C_{\mathrm{rob}}(\psi,\mathbf{E}) = \max_{X\geq 0, X_{i,i}=\mathbb{1}} \sum_{i\neq j} \mathrm{tr}(X_{j,i}A_i|\psi\rangle\langle\psi|A_j^\dagger)$. Hence, it follows that

$$\begin{aligned} C_{\mathrm{rob}}(\psi,\mathbf{E}) &\geq \sum_{i\neq j} \mathrm{tr}(\tilde{X}_{j,i}A_i|\psi\rangle\langle\psi|A_j^\dagger) \\ &= \sum_{i\neq j} \sqrt{p_i p_j}\,\mathrm{tr}(|\phi_j\rangle\langle\phi_i|\,|\phi_i\rangle\langle\phi_j|) \\ &= \sum_{i\neq j} \sqrt{p_i p_j}. \end{aligned} \tag{B6}$$

By comparing (B4) and (B6), we infer that $C_{\mathrm{rob}}(\psi,\mathbf{E}) \geq C_{\ell_1}(\psi,\mathbf{E})$ holds for any pure state ψ. Combining this with the inequality $C_{\mathrm{rob}}(\rho,\mathbf{E}) \leq C_{\ell_1}(\rho,\mathbf{E})$ for general states ρ, we conclude that $C_{\mathrm{rob}} = C_{\ell_1}$ holds for pure states and any POVM. □

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Physical Review Letters **98**, 230501 (2007).
[2] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nature Communications **9**, 459 (2018).
[3] F. G. S. L. Brandão and G. Gour, Physical Review Letters **115**, 070503 (2015).
[4] Z.-W. Liu, X. Hu, and S. Lloyd, Physical Review Letters **118**, 060502 (2017).
[5] E. Chitambar and G. Gour, Reviews of Modern Physics **91**, 025001 (2019).
[6] M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen De, U. Sen, et al., Physical Review Letters **90**, 100402 (2003).
[7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Reviews of Modern Physics **81**, 865 (2009).
[8] M. Horodecki, P. Horodecki, and J. Oppenheim, Physical Review A **67**, 062104 (2003).
[9] I. Marvian and R. W. Spekkens, New Journal of Physics **15**, 033001 (2013).
[10] I. Marvian and R. W. Spekkens, Nature communications **5**, 3821 (2014).
[11] F. G. S. L. Brandao, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Physical Review Letters **111**, 250404 (2013).
[12] T. Baumgratz, M. Cramer, and M. B. Plenio, Physical Review Letters **113**, 140401 (2014).
[13] A. Winter and D. Yang, Physical Review Letters **116**, 120404 (2016).
[14] A. Streltsov, G. Adesso, and M. B. Plenio, Reviews of Modern Physics **89**, 041003 (2017).
[15] B. Coecke, T. Fritz, and R. W. Spekkens, Information and Computation **250**, 59 (2016).
[16] M. Horodecki and J. Oppenheim, International Journal of Modern Physics B **27**, 1345019 (2013).
[17] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Physical Review Letters **115**, 020403 (2015).
[18] H. Kwon, H. Jeong, D. Jennings, B. Yadin, and M. S. Kim, Physical Review Letters **120**, 150602 (2018).
[19] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Physical Review Letters **119**, 190501 (2017).
[20] F. Bischof, H. Kampermann, and D. Bruß, arXiv:1812.00018 (2018).
[21] J. Åberg, arXiv:quant-ph/0612146 (2006).
[22] M. Piani, M. Cianciaruso, T. R. Bromley, C. Napoli, N. Johnston, and G. Adesso, Physical Review A **93**, 042107 (2016).
[23] G. Gour, I. Marvian, and R. W. Spekkens, Physical Review A **80**, 012307 (2009).
[24] I. Marvian, R. W. Spekkens, and P. Zanardi, Physical Review A **93**, 052331 (2016).
[25] I. Marvian and R. W. Spekkens, Physical Review A **94**, 052324 (2016).

[26] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Journal of Physics A: Mathematical and General **38**, 5979 (2005).

[27] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Physical Review A **92**, 022124 (2015).

[28] X. Yuan, Q. Zhao, D. Girolami, and X. Ma, arXiv:1605.07818 (2016).

[29] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Transactions on Information Theory **55**, 5840 (2009).

[30] R. Renner, International Journal of Quantum Information **6**, 1 (2008).

[31] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[32] Z. Cao, H. Zhou, and X. Ma, New Journal of Physics **17**, 125011 (2015).

[33] F. Bischof, H. Kampermann, and D. Bruß, Physical Review A **95**, 062305 (2017).

[34] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Physical Review Applied **7**, 054018 (2017).

[35] M. Ioannou, J. B. Brask, and N. Brunner, Physical Review A **99**, 052338 (2019).

[36] C. Napoli, T. R. Bromley, M. Cianciaruso, M. Piani, N. Johnston, and G. Adesso, Physical Review Letters **116**, 150502 (2016).

[37] K. Bu, U. Singh, S.-M. Fei, A. K. Pati, and J. Wu, Physical Review Letters **119**, 150405 (2017).

[38] J. Löfberg, in *In Proceedings of the CACSD Conference* (Taipei, Taiwan, 2004).

[39] K. Bu and C. Xiong, Quantum Information & Computation **17**, 1206 (2017).

[40] S. Rana, P. Parashar, A. Winter, and M. Lewenstein, Physical Review A **96**, 052336 (2017).

[41] A. E. Rastegin, Journal of Physics A: Mathematical and Theoretical **51**, 414011 (2018).

[42] E. Chitambar and G. Gour, Physical Review A **94**, 052336 (2016).

[43] E. Chitambar and G. Gour, Physical Review Letters **117**, 030401 (2016).

[44] B. Yadin, J. Ma, D. Girolami, M. Gu, and V. Vedral, Physical Review X **6**, 041028 (2016).

[45] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and X. Ma, Physical Review Letters **120**, 070403 (2018).

[46] B. Regula, K. Fang, X. Wang, and G. Adesso, Physical Review Letters **121**, 010401 (2018).

[47] L. Lami, arXiv:1902.02427 (2019).

[48] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and A. Winter, IEEE Transactions on Information Theory **1** (2019).

[49] L. Lami, B. Regula, and G. Adesso, Physical Review Letters **122**, 150402 (2019).

[50] A. Streltsov, H. Kampermann, S. Wölk, M. Gessner, and D. Bruß, New Journal of Physics **20**, 053058 (2018).

[51] J. Watrous, *The theory of quantum information* (Cambridge University Press, 2018).

APPENDIX B

Matlab Source Codes

The Matlab files below make use of the toolbox QETLAB, which is freely available at: www.qetlab.com. Moreover, all files involving semidefinite programming require the Matlab toolbox YALMIP [Löf04], which is freely available at: yalmip.github.io. Moreover, these require the SDP solver SDPT3 [TTT99].

Construction of minimal Naimark Extension

```
% This is MinNaimark.m

% Input: a POVM E in the form of an array, i.e., the i-th effect is
    given by E(:,:,i)

% Output: the minimal Naimark extension Pmin of E in the form of an
    array


function [Pmin] = MinNaimark(E)
dim = size(E,1);
m = size(E,3);

% Identity
Id = eye(dim);
for i=1:dim
    c(:,i)=Id(:,i);
end


% Check POVM properties
for i=1:m
    if any(eig(E(:,:,i)))<-1e-9 % nonnegative effects
        disp('POVM not positive')
        return
    end
end
if norm(sum(E,3)-Id)>1e-9 % normalized POVM
        disp('POVM not normalized')
        return
end
```

```
30
31
32 % Calculate Rank of POVM effects
33 for i=1:m
34     r(i) = rank(E(:,:,i),1e-8); % 1e-8 is rank tolerance
35 end
36 dmin = sum(r); % outcome number of fine-grained POVM
37
38
39 % Identities and bases
40 Idn = eye(dmin);
41 for i=1:dmin
42     cn(:,i)=Idn(:,i);
43 end
44
45
46 % Compute eigenvectors with nonzero eigenvalue of effects
47 for i=1:m
48     [eigvec{i},lambda{i}] = eig(E(:,:,i));
49     [lambdasort{i},ind{i}] = sort(diag(lambda{i}));
50     eigvecsort{i} = eigvec{i}(:,ind{i}); % sort in ascending order
51 end
52
53
54 % Determine measurement directions of the fine-grained POVM
55 f=0;
56 for i=1:m
57     for k=(dim-r(i)+1):dim % only use the eigenvectors of nonzero
          eigenvalue
58         f = f+1;
59         psi(:,f) = sqrt(lambdasort{i}(k))*eigvecsort{i}(:,k);
60     end
61 end
62
63
64 % Isometry matrix, with measurement directions as rows
65 for i=1:dmin
66     for j=1:dim
67 Psi(i,j) = dot(c(:,j),psi(:,i));
68     end
69 end
70
71
72 % Extend isometry to unitary
73 Orthocompl = null(Psi');
74 Psi = [Psi,Orthocompl];
75
76
77 % Naimark measurement directions are ROWS of Unitary
```

```
78  for i=1:dmin
79      phi(:,i) = Psi(i,:);
80  end
81
82
83  % Minimal Naimark extension effects
84  f=1;
85  for i=1:m
86      for k=f:f+r(i)-1
87          if k==f
88              Pmin(:,:,i) = phi(:,k)*phi(:,k)';
89          else
90              Pmin(:,:,i) = Pmin(:,:,i) + phi(:,k)*phi(:,k)';
91          end
92      end
93      f=f+r(i);
94  end
95
96
97  % Check for correct Naimark extension
98  for i=1:m
99      if norm(sum(Pmin,3)-eye(dmin))>1e-9 % normalization
100         disp('NE not normalized')
101         return
102     end
103 end
104 for i=1:m
105     if norm(Pmin(:,:,i)^2-Pmin(:,:,i))>1e-9 % idempotent
106         disp('NE not idempotent')
107         return
108     end
109 end
110 for i=1:m
111     for j=1:i-1
112         if norm(Pmin(:,:,i)*Pmin(:,:,j))>1e-9 % orthogonal
113         disp('NE not orthogonal')
114         return
115         end
116     end
117 end
118 for i=1:m
119     if norm(E(:,:,i)-Pmin(1:dim,1:dim,i))>1e-9 % extension
120     disp('NE not proper extension')
121     return
122     end
123 end
124
125 return
```

Relative Entropy of POVM-based Coherence

```
% This is RelEntPBC.m

% Input: a quantum state rho AND a POVM E in the form of an array, i
    .e., the i-th effect is given by E(:,:,i)

% Output: the Relative Entropy of POVM-based coherence of rho given
    E


function [Coh] = RelEntPBC(rho,E)

dim = length(rho);
m = size(E,3);


% Compute Measurement operator from POVM
A = zeros(dim,dim,m);
for i=1:m
    A(:,:,i)=sqrtm(E(:,:,i));
end


% Compute Relative Entropy of PB Coherence via QETLAB vN Entropy
for i=1:m
    if (i==1)
        Sum = Entropy(A(:,:,i)*rho*A(:,:,i)');
    else
        Sum = Sum + Entropy(A(:,:,i)*rho*A(:,:,i)');
    end
end

Coh = Sum - Entropy(rho);

return
```

ℓ_1-norm of POVM-based Coherence

```
% This is L1NormPBC.m

% Input: a quantum state rho AND a POVM E in the form of an array, i
    .e., the i-th effect is given by E(:,:,i)

% Output: the l1-norm of POVM-based coherence of rho given E


function [Coh] = L1NormPBC(rho,E)

dim = length(rho);
m = size(E,3);


% Compute Measurement operator from POVM
A = zeros(dim,dim,m);
for i=1:m
    A(:,:,i)=sqrtm(E(:,:,i));
end


% Compute Relative Entropy of PB Coherence via QETLAB vN Entropy
for i=1:m
    for j=1:m
        if (i==1&&j==1)
            Sum = 0;
        elseif (i~=j)
            Sum = Sum + TraceNorm(A(:,:,i)*rho*A(:,:,j)'); % Trace
                Norm
            %Sum = Sum + norm(A(:,:,i)*rho*A(:,:,j)',inf); %
                Infinity Norm
        end
    end
end

Coh = Sum;

return
```

Robustness of POVM-based Coherence

```
% This is RobPBC.m

% Input: a quantum state rho AND a POVM E in the form of an array, i.e., the i-th effect is given by E(:,:,i)

% Output: the Robustness of POVM-based coherence of rho given E


function [Coh] = RobPBC(rho,E)

dim = length(rho);
m = size(E,3);


% Matrix Units
Idm = eye(m);
for i=1:m
    c(:,i)=Idm(:,i);
end
for i=1:m
    for j=1:m
mu(:,:,i,j) = c(:,i)*c(:,j)'; % Matrix canonical basis in lexicographical order
    end
end


% Compute Measurement operators from POVM
A = zeros(dim,dim,m);
for i=1:m
    A(:,:,i)=sqrtm(E(:,:,i));
end


% Variable and Objective
for i = 1:m
    X{i} = sdpvar(dim,dim,'hermitian','complex');
end

for i=1:m
    if i==1
        Objective = trace(X{i});
    else
        Objective = Objective + trace(X{i});
    end
end

```

```
46
47 % Constraint
48 for i=1:m
49     for j=1:m
50         if i==j
51             sigma{i,j} = X{i};
52         else
53             sigma{i,j} = -A(:,:,i)*rho*A(:,:,j)';
54         end
55     end
56 end
57
58 for i=1:m
59     for j=1:m
60         if (i==1 && j==1)
61             Sum = kron(sigma{i,j},mu(:,:,i,j));
62         else
63             Sum = Sum + kron(sigma{i,j},mu(:,:,i,j));
64         end
65     end
66 end
67
68 Constraints = [Sum >= 0];
69
70 Options = sdpsettings ('verbose',2,'cachesolver',1,'showprogress'
       ,1,...
71  'solver','sdpt3','savesolveroutput',1);
72
73 sol = optimize(Constraints,Objective,Options);
74
75 Coh = value(Objective)
76
77 return
```

Check whether a given Channel is POVM-incoherent (MPI)

```
% This is IsMPI.m

% Input: a channel "Channel" given as a matrix in the standard
    matrix basis AND a POVM E in the form of an array, i.e., the i-
    th effect is given by E(:,:,i)

% Output: a string indicating whether the input channel is (
    maximally) POVM-incoherhent MPI


function [ChannelIsMPI] = IsMPI(Channel,E)

dim = size(E,1);
m = size(E,3);
Pmin = MinNaimark(E);
dmin = size(Pmin,1);
dn = dmin;


% Identity and basis
Idn = eye(dn);
for i=1:dn
    cn(:,i)=Idn(:,i);
end
% Identity
Id = eye(dim);
for i=1:dim
    c(:,i)=Id(:,i);
end

for i=1:dn
    for j=1:dn
Bh(:,:,j,i) = cn(:,i)*cn(:,j)'; % Matrix canonical basis in
    lexicographical order
    end
end
B = reshape(Bh(:,:,:,:),[dn dn dn^2]);


% Extract basis elements belonging to the system basis
for i=1:dim
    for j=1:dim
        Blh(:,:,j,i) = cn(:,i)*cn(:,j)';
    end
end
Bl = reshape(Blh(:,:,:,:),[dn dn dim^2]);
for i=1:dim^2
```

```
    Blv(:,i) = reshape(transpose(Bl(:,:,i)),[dn^2 1]);
end


% POVM from Naimark extension
for i=1:m
    E(:,:,i) = Pmin(1:dim,1:dim,i);
end


% SDP variable
Choi = sdpvar(dn^2,dn^2,'hermitian','complex');


% Derive process (transfer) matrix from Choi matrix
for i=1:dn^2
    if i==1
        Trans = kron(Idn,B(:,:,i))*Choi*kron(B(:,:,i),Idn);
    else
        Trans = Trans + kron(Idn,B(:,:,i))*Choi*kron(B(:,:,i),Idn);
    end
end

Trans = dn*Trans; % Renormalization, because Choi has trace one for
    channel


% Measurement map is equal to primal feasible map
for i=1:dim^2
    for j=1:dim^2
          Translocal(i,j) = Blv(:,i)'*Trans*Blv(:,j);
    end
end
Equality = [Channel==Translocal];


% 0. Constraint: completely positive and trace preserving
CPTP = [Choi>=0, PartialTrace(Choi,1)==Idn/dn];


% 1. Constraint: Naimark incoherent
% Action of Naimark-dephasing operator on matrix basis
for i=1:dn^2
    for k=1:m
        if (k==1)
            Delta(:,:,i) = Pmin(:,:,k)*B(:,:,i)*Pmin(:,:,k);
        else
            Delta(:,:,i) = Delta(:,:,i) + Pmin(:,:,k)*B(:,:,i)*Pmin
                (:,:,k);
```

```
91          end
92      end
93  end
94
95
96  % Transfer matrix of dephasing operator
97  Deltat=zeros(dn^2,dn^2);
98  for i=1:dn^2
99      for j=1:dn^2
100         Deltat(i,j) = trace(B(:,:,i)'*Delta(:,:,j));
101     end
102 end
103
104
105 % 2. Constraint: subspace preserving
106 PiL = blkdiag(Id,zeros(dn-dim)); % Projector onto local subspace
107 % Transfer matrix of local subchannel projection L
108 Lt=zeros(dn^2,dn^2);
109 for i=1:dn^2
110     for j=1:dn^2
111         Lt(i,j) = trace(B(:,:,i)'*PiL*B(:,:,j)*PiL);
112     end
113 end
114
115 Sub = [Trans*Lt==Lt*Trans*Lt]; % subspace-preserving operation
116 Inc = [Trans*Deltat*Lt==Deltat*Trans*Deltat*Lt]; % Incoherent
        operation
117
118
119 % SDP optimization
120 Constraints = [Equality,CPTP,Inc,Sub];
121
122 Options = sdpsettings ('verbose',2,'cachesolver',1,'showprogress',1,
        'debug',1,...
123  'solver','sdpt3','savesolveroutput',1,'allownonconvex',1,'debug',1)
         ;
124
125 sol=optimize(Constraints,[],Options);
126
127 error=1e-6;
128 if (sol.problem==0||sol.problem==5||sol.problem==4&&sol.solveroutput
        .info.relgap<1e-3) %not for SEDUMI
129   disp('SDP converged')
130   Trans = value(Trans);
131   Choi = value(Choi);
132   Translocal = value(Translocal);
133   % no square root for this fidelity
134   % check whether map is CPTP
135    if (norm(PartialTrace(Choi,1)-Idn/dn)>error||any(eig(Choi)<-error
```

```
        ))
136     disp('Channel not CPTP')
137 %    Fidelity=-1;
138     return
139    end
140    for i=1:100 % Check whether channel is really POVM-incoherent
141        check{i} = RandomDensityMatrix(dim);
142        checkv{i} = reshape(transpose(check{i}),[dim^2 1]);
143        Imcheckv{i} = Translocal*checkv{i};
144        Imcheck{i} = transpose(reshape(Imcheckv{i},[dim dim]));
145        if RelEntPBC(Imcheck{i},E)-RelEntPBC(check{i},E)>=1e-6
146            disp('Input Map not incoherent')
147            CohIncrease = abs(RelEntPBC(Imcheck{i},E)-RelEntPBC(check{
                    i},E))
148            return
149        elseif abs(trace(Imcheck{i})-1)>=1e-5
150            disp('Test: Channel not TP')
151            return
152        else
153            continue
154        end
155    end
156 %    if norm(M-MA)>1e-4
157 %        disp('consistency check failed')
158 %        return
159 %    end
160    disp('Map passed CPTP and MIO Test')
161    disp('Channel is POVM-incoherent')
162    ChannelIsMPI = true;
163 else
164    disp('optimization problem:')
165   yalmiperror(sol.problem)
166   ChannelIsMPI = false;
167   return
168 end
```

Maximal Fidelity between two states under MPI operations

```
% This is Fmax.m

% The program computes the maximal Fidelity between two states achievable by POVM-incoherent operations MPI

% Input: an initial state I AND a target state T AND a POVM E in the form of an array, i.e., the i-th effect is given by E(:,:,i)

% Output: the quantum fidelity between T and MPI[I] optimized over all MPI operations of the POVM E


function [Fidelity] = Fmax(I,T,E)

dim = size(E,1);
m = size(E,3);
Pmin = MinNaimark(E);
dn = size(Pmin,1);


% Auxiliary definitions
Id = eye(dim);

Idn = eye(dn);
for i=1:dn
    cn(:,i)=Idn(:,i);
end

for i=1:dn
    for j=1:dn
Bh(:,:,j,i) = cn(:,i)*cn(:,j)'; % Matrix canonical basis in lexicographical order
    end
end
B = reshape(Bh(:,:,:,:),[dn dn dn^2]);


% SDP Variables
Choi = sdpvar(dn^2,dn^2,'hermitian','complex'); % Choi matrix on Naimark space
X = sdpvar(dim,dim,'full','complex'); % Auxiliary variable for Fidelity


% Derive Process (transfer) matrix from Choi matrix
for i=1:dn^2
    if i==1
```

```
42          Trans = kron(Idn,B(:,:,i))*Choi*kron(B(:,:,i),Idn);
43      else
44          Trans = Trans + kron(Idn,B(:,:,i))*Choi*kron(B(:,:,i),Idn);
45      end
46  end
47
48  Trans = dn*Trans; % Renormalization, because Choi has trace one for
        channel
49
50
51  % 0. Constraint: completely positive and trace preserving
52  CPTP = [Choi>=0, PartialTrace(Choi,1)==Idn/dn];
53
54
55  % 1. Constraints: Naimark incoherent
56  % Dephasing operator on matrix basis
57  for i=1:dn^2
58      for k=1:m
59          if (k==1)
60              Delta(:,:,i) = Pmin(:,:,k)*B(:,:,i)*Pmin(:,:,k);
61          else
62              Delta(:,:,i) = Delta(:,:,i) + Pmin(:,:,k)*B(:,:,i)*Pmin
                    (:,:,k);
63          end
64      end
65  end
66
67
68  % Transfer (process) matrix of dephasing operator
69  Deltat=zeros(dn^2,dn^2);
70  for i=1:dn^2
71      for j=1:dn^2
72          Deltat(i,j) = trace(B(:,:,i)'*Delta(:,:,j));
73      end
74  end
75
76
77  % 2. Constraint: subspace preserving
78  PiL = blkdiag(Id,zeros(dn-dim)); % Projector onto local subspace
79  % Transfer matrix of projection onto local operators
80  Lt=zeros(dn^2,dn^2);
81  for i=1:dn^2
82      for j=1:dn^2
83          Lt(i,j) = trace(B(:,:,i)'*PiL*B(:,:,j)*PiL);
84      end
85  end
86
87  Sub = [Trans*Lt==Lt*Trans*Lt]; % subspace-preserving operation
88  Inc = [Trans*Deltat==Deltat*Trans*Deltat]; % MIO operation
```

```
89
90
91  % Correct representation for transfer matrix
92  In = blkdiag(I,zeros(dn-dim));
93  Iv = reshape(transpose(In),[dn^2 1]); % vectorization, transpose
        necessary
94  % for lexicographical ordering
95
96  % Mapping by multiplying transfer matrix
97  Mv = Trans*Iv; % vector after map
98  Mn = transpose(reshape(Mv,[dn dn])); % transpose necessary
99  M = Mn(1:dim,1:dim); % state after map
100
101 % MA needs to coincide with M if everything is consistent
102 MAn = dn*PartialTrace(Choi*kron(Idn,transpose(In)),2);
103 MA = MAn(1:dim,1:dim); % state after map
104
105
106 % FIDELITY FUNCTION CONSTRAINT
107 Y = [T X;X' M];
108 FidP = [Y>=0];
109
110
111 % SDP optimization
112 Constraints = [CPTP,Inc,Sub,FidP];
113
114
115 % Maximizing function: Fidelity
116 %Fidelity = trace(Tn*Mn);
117 Fidelity = 1/2*(trace(X)+trace(X'));
118
119
120 Options = sdpsettings ('verbose',2,'cachesolver',1,'showprogress',1,
        'debug',1,...
121  'solver','sdpt3','savesolveroutput',1,'allownonconvex',1,'debug',1)
        ;
122
123 sol=optimize(Constraints,-Fidelity,Options);
124
125
126 % Extract optimized parameters
127 Channel = value(Trans);
128 Choi = value(Choi);
129 M = value(M);
130 MA = value(MA);
131
132
133 error=1e-9;
134 if (sol.problem==0||sol.problem==5||sol.problem==4&&sol.solveroutput
```

```
    .info.relgap<1e-3)
  disp('SDP converged')
  % no square root for this fidelity
        Fidelity=value(Fidelity)
  % check whether map is CPTP
  if (abs(trace(M)-1)>error||any(eig(M)<-error))
  disp('Channel not CPTP')
  Fidelity=-1;
  return
  end
  for i=1:100 % Check whether channel is really POVM-incoherent
      check{i}=RandomDensityMatrix(2);
      checkn{i} = blkdiag(check{i},zeros(dn-dim));
      checkv{i} = reshape(checkn{i},[dn^2 1]);
      Imcheckv{i} = Channel*checkv{i};
      Imcheckn{i} = reshape(Imcheckv{i},[dn dn]);
      Imcheck{i} = Imcheckn{i}(1:dim,1:dim);
      if RelEntPBC(Imcheck{i},E)-RelEntPBC(check{i},E)>=1e-9
          disp('Channel not incoherent')
          CohIncrease = RelEntPBC(Imcheck{i},E)-RelEntPBC(check{i},E
              )
          Fidelity=-1;
          break
      else
          continue
      end
  end
  if norm(M-MA)>1e-4
      disp('consistency check failed')
      return
  end
  disp('Map passed CPTP and MIO Test')
else
  disp('optimization problem:')
 yalmiperror(sol.problem)
 return
end


return
```

APPENDIX C

Eidesstattliche Versicherung

Ich versichere an Eides Statt, dass die Dissertation von mir selbständig und ohne unzulässige fremde Hilfe unter Beachtung der „Grundsätze zur Sicherung guter wissenschaftlicher Praxis an der Heinrich-Heine-Universität Düsseldorf“ erstellt worden ist.

Ort, Datum: _____

Unterschrift: _____