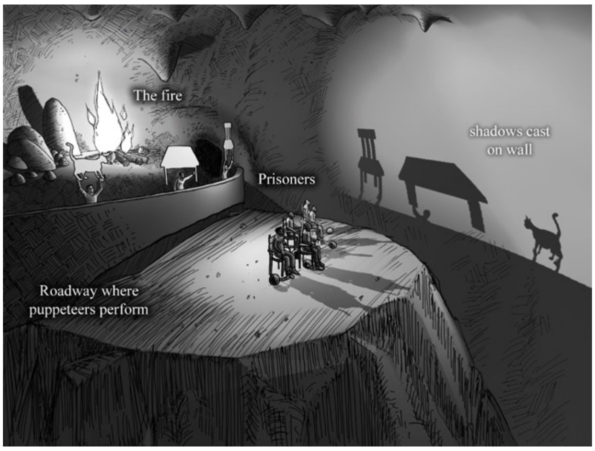
Calculating and Bounding POVM Norm Constants

Richard Küng*

July 13, 2012

This master thesis was developed in the research group of Prof. Dr. Matthias Christandl under the supervision of Dr. Frédéric Dupont-Dupuis at ETH Zürich.



Abstract

The main objective of this thesis are POVM-norm constants. Such constants allow for comparing the optimal bias achievable by an actual POVM measurement to Helstrom's ideal one. We present two novel methods of calculating or at least bounding these constants. Our methods are universally applicable and use well established computational concepts such as semidefinite programming and computational geometry. This allows for an explicit implementation of our algorithms. One method is particularly well suited for the special case of exactly informationally complete POVMs (e.g SIC-POVMs) for which explicit constants can be readily obtained.

*e-mail: kuengr@ethz.ch

I dedicate this thesis to my family – Erik, Felix, Gabriela and Josef Küng – who has always supported me and encouraged me to never stop being curious.

Richard Küng

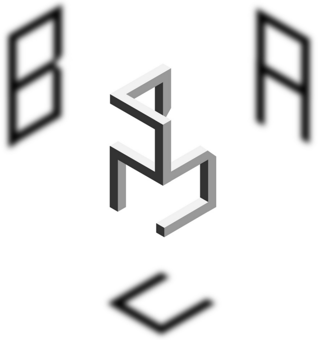


Figure 1: This *ABC triplet ambigram* illustrates how a single object can cast various kinds of shadows. The shadow's form solely depends on the position of the light source. The graphic has been taken from [2].

Abstract

The sketch on the cover illustrates Plato's *allegory of the cave*. In his dialog Politeia (the Republic) the protagonist Socrates introduces the following Gedankenexperiment. A group of people (prisoners) have spent their entire life at the bottom of a cave. By chains they are forced to face the cave's wall without being able to turn around. Hence, they cannot see the large fire burning behind their backs. They only see its reflection on the wall in front of them. Between the fire and the prisoners there is a roadway passing. Along this path, people (puppeteers) carrying various things walk by. The carried objects cast shadows on the cave's wall. The prisoners can watch these shadows, but are not aware of their origin. Since these people cannot see anything else, the shadows – and not their origin – constitute reality for them.

Plato uses this allegory in order to illustrate his concept of "platonic ideas". In my opinion, this setting also illustrates the limitations of quantum mechanical experiments very well. Measuring a quantum state allows us to access the state's probability outcome vector and not the state itself. This situation strongly resembles the allegory of the cave. Through an experiment, we can only see the a shadow of the state, not the state itself. Consequently, the question of quantum state discrimination corresponds to recognizing an object by only having access to some shadow that it casts. This task is obviously more difficult than recognizing the original object directly. In addition, it strongly depends on the position of the light source (or equivalently: the shadow's form). Figure 1 illustrates how one object can indeed cast various types of shadows. Norm constants – the main objective of this thesis – allow for quantifying this recognition difficulty for arbitrary "light source positions" (experiments) by comparing it to the difficulty of recognizing the original object. I consider this allegory to be very illustrative and beautiful which is why I decided to start my thesis with it.

Contents

1 Introduction

The scope of this thesis is *state discrimination*, where one aims to distinguish two quantum states ρ and σ with high probability. At the very heart of this field lies Helstrom's theorem [3] which states that the minimal error probability of any discrimination procedure is given by $P_E^{\text{Helstrom}} = \frac{1}{2} - \frac{1}{4}\|\rho - \sigma\|_1$. Here $\|.\|_1$ denotes the trace norm. This corresponds to an optimal bias of

$$\beta_{\text{Helstrom}} = \frac{1}{2}\|\rho - \sigma\|_1,$$

provided that any physical measurement can be implemented. In all practical situations this ideal requirement cannot be met. It is therefore natural to consider the situation, where we want to do state discrimination using non-universal measurement devices. In particular, let us assume that we only have access to one measurement apparatus that is given by a single informationally complete POVM $\{M_k\}_{k=1}^n$. Therefore, the only way to access our states ρ and σ is via our measurement $\{M_k\}_{k=1}^n$. We can formulate this situation mathematically by identifying the measurement procedure with a linear mapping

$$\begin{aligned} \mathcal{M}:\ D(\mathcal{X}) &\rightarrow \mathbb{R}_+^n, \\ \rho &\mapsto \sum_{k=1}^n |k\rangle \mathrm{tr}\left(M_k \rho\right) \end{aligned}$$

This function maps density operators onto probability outcome vectors. Our measurement device only provides access to the vectors $p = \mathcal{M}(\rho)$ and $q = \mathcal{M}(\sigma)$. The optimal bias achievable for distinguishing these vectors is given by the maximum likelihood rule and amounts to

$$\beta_{\mathcal{M}} = \frac{1}{2}\|p - q\|_{l_1} = \frac{1}{2}\|\mathcal{M}(\rho - \sigma)\|_{l_1},$$

where $\|.\|_{l_1}$ denotes the l_1-norm. It is natural to compare this actual bias to Helstrom's ideal one. One way of doing so is to search for constants $\lambda, \mu > 0$ that allow for relating both biases via an inequality chain

$$\lambda\|\rho - \sigma\|_1 \leq \|\mathcal{M}(\rho - \sigma)\|_1 \leq \mu\|\rho - \sigma\|_1 \quad \forall \rho, \sigma \in D(\mathcal{X}).$$

Note that the difference of arbitrary quantum states corresponds to an arbitrary (bounded) traceless hermitian operator. Thus we can rewrite this sandwich inequality:

$$\lambda\|X\|_1 \leq \|\mathcal{M}(X)\|_1 \leq \mu\|X\|_1 \quad \forall X \in \mathrm{Herm}(\mathcal{X}) \text{ with } \mathrm{tr}(X) = 0. \tag{1}$$

Omitting the tracelessness requirement yields another inequality relation with looser bounds $\tilde{\lambda}$ and $\tilde{\mu}$:

$$\tilde{\lambda}\|X\|_1 \leq \|\mathcal{M}(X)\|_1 \leq \tilde{\mu}\|X\|_1 \quad \forall X \in \mathrm{Herm}(\mathcal{X}). \tag{2}$$

Note that obviously $\tilde{\lambda} \leq \lambda$ and $\mu \leq \tilde{\mu}$. W. Matthews, S. Wehner and A. Winter introduced the traceless version of this quantity in [4] and pointed out that the bounded object actually does constitute a norm

$$\|X\|_{\mathcal{M}} := \|\mathcal{M}(X)\|_1 \quad \forall X \in \mathrm{Herm}(\mathcal{X})$$

on the finite dimensional vector space $\mathrm{Herm}(\mathcal{X})$. From this point of view, statement (2) is nothing but the fundamental fact that all norms are equivalent on finite dimensional vector spaces. In particular, this implies that the constants $\tilde{\lambda}$ and $\tilde{\mu}$ (and thus λ and μ as well) are nontrivial. W. Matthews and his collaborators could show that the constant λ in (1) is furthermore related to its analogue $\tilde{\lambda}$ in (2) via

$$\frac{1}{2}\lambda \leq \tilde{\lambda} \leq \lambda. \tag{3}$$

Therefore these two constants are equivalent up to a multiplicative factor of 2. In addition, the relation $\mu \leq \tilde{\mu} \leq 1$ obviously holds. We present a novel geometric and intuitive proof of relation (3) in subsection 4.2.5.

The constants λ and μ have operational significance due to relation (1). Indeed they relate the optimal measurement bias $\beta_{\mathcal{M}}$ to the universally optimal Helstrom bias $\beta_{\mathrm{Helstrom}}$.

- The constant λ can be interpreted as a *worst case promise* for the measurement $\mathcal{M}$: For any two states $\rho, \sigma \in D(\mathcal{X})$, the optimal measurement bias $\beta_{\mathcal{M}}$ is at least λ-times as well as the Helstrom bias $\beta_{\mathrm{Helstrom}}$.

- The constant μ serves as a *bound on optimal performance*: For any two states $\rho, \sigma \in D(\mathcal{X})$ the optimal measurement bias $\beta_{\mathcal{M}}$ is at most μ-times as well as $\beta_{\mathrm{Helstrom}}$(where $\mu \leq 1$).

Such a worst case promise λ is particularly important for the universally applicable measurements that various types of quantum state tomography [5, 6] predict. Hence, it is natural to look for procedures that permit calculating – or at least bounding – such norm constants efficiently. This is precisely the scope of our work. First steps into this direction were done by W. Matthews et al, who analytically obtained bounds for the uniform POVM, 4- and 2-designs as well as PPT and separable measurements in [4]. Their result for the uniform POVM implies that λ is upper bounded by a dimensional factor proportional to $\frac{1}{\sqrt{d}}$, where $d = \dim \mathcal{X}$. Therefore the norm constants λ and $\tilde{\lambda}$ necessarily depend on the dimension of the considered Hilbert space.

Apart from this, the authors are only aware of one other approach by D. Reeb, M. J. Kastoryano and M. Wolf [7]. In their paper, the authors use Hilbert's projective metric in order to get a potentially nontrivial bound on μ for arbitrary POVM measurements. This metric is mathematically beautiful and highly relevant as a theoretical tool, but has the drawback of seeming to be hard to compute efficiently in many situations.

We present a different approach using polytope theory, quantum channel concepts and semidefinite programming.

For the sake of self-completeness, we devote chapter 2 to introducing the mathematical and physical concepts that are important for our work.

Our approaches extensively use concepts from convex geometry. For this reason we give an introduction to convexity in chapter 3.

In chapter 4 we present our contribution. The concepts of POVM norms and POVM norm constants are properly defined in subsection 4.1. We furthermore introduce an important auxiliary tool – inverse measurement mappings.
In section 4.2 we introduce our first approach which is of geometric nature. It uses the fact that convex maximization over convex polytopes corresponds to checking the function's value at all the polytope's vertices. This can be done efficiently, provided that the number of vertices is not too large. Such a procedure allows for evaluating $\tilde{\lambda}$ and λ efficiently for exactly informationally complete measurements. SIC POVMs constitute a subfamily of such measurements that are endowed with an additional symmetry property. This symmetry allows us to calculate λ and $\tilde{\lambda}$ explicitly for arbitrary SIC POVMs. This result is original and refines the bound presented in [4]. For a general POVM measurement, a similar reasoning yields upper and lower bounds on the norm constants that can be efficiently calculated. For obvious reasons, we call this procedure as *polytope approach*.
In section 4.3 we present another approach, dubbed the *diamond approach*. It is obtained by interpreting the measurement $\mathcal{M}$ as a channel. This allows for relating the norm constants λ and μ to induced 1-norms of particular superoperators Φ_λ and Φ_μ. We give an explicit construction of these superoperators that solely depends on $\{M_k\}_k$. Since the induced 1-norm seems to be hard to compute, we use the diamond norm as a computationally efficient proxy. This yields a nontrivial lower bound on λ and a (possibly trivial) upper bound on μ as well as a new interpretation for the diamond norm in terms of convex relaxations.

We conclude our thesis with a summary (Chapter 5) and an appendix containing a simple 1 qubit example calculation.

2 Mathematical and physical background

2.1 Basic notation and concepts

In our thesis we largely adopt Watrous notation [8, 9, 10, 11] for complex vector spaces, operators and superoperators. The following summary of basic concepts mainly contains material from eaedem sources.

2.1.1 States

The letters $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ and $\mathcal{W}$ denote complex vector spaces of the form $\mathbb{C}^n$ for some $n \in \mathbb{N}$. Their elements are identified with n-dimensional column vectors.

For two such vectors $x, y \in \mathcal{X} \simeq \mathbb{C}^n$ we define the standard inner product as

$$\langle x, y \rangle = \sum_{i=1}^{n} \bar{x}_i y_i,$$

where the bar denotes complex conjugation. Using this scalar product, we define the Euclidean norm as

$$\|x\|_2 = \sqrt{\langle x, x \rangle}$$

for any $x \in \mathcal{X}$. We denote the unit sphere in $\mathcal{X}$

$$S(\mathcal{X}) = \{x \in \mathcal{X} : \|x\|_2 = 1\},$$

and call the j-th standard vector in $\mathcal{X}$ e_j.

2.1.2 Operators

For $\mathcal{X} = \mathbb{C}^n$ and $\mathcal{Y} = \mathbb{C}^m$ the complex vector space consisting of all linear mappings $A : \mathcal{X} \to \mathcal{Y}$ is denoted $L(\mathcal{X}, \mathcal{Y})$. Such mappings are called operators. We identify this space with the space of complex $n \times m$-matrices in the usual way. For automorphisms $L(\mathcal{X}, \mathcal{X})$ we use the shorthand notation $L(\mathcal{X})$. the identity operator on $L(\mathcal{X})$ is called $\mathbb{I}_{\mathcal{X}}$. For each $A \in L(\mathcal{X}, \mathcal{Y})$ we define the adjoint operator $A^* \in L(\mathcal{Y}, \mathcal{X})$ to be the unique operator that satisfies

$$\langle x, Ay \rangle = \langle A^* x, y \rangle \quad \forall x, y \in \mathcal{X}.$$

The Hilbert-Schmidt product on $L(\mathcal{X}, \mathcal{Y})$ is defined as

$$\langle A, B \rangle = \operatorname{tr}(A^* B) \quad \forall A, B \in L(\mathcal{X}, \mathcal{Y}),$$

where $\operatorname{tr} : L(\mathcal{Y}) \to \mathbb{C}$ denotes the trace operator. By identifying any vector $x \in \mathcal{X}$ with the linear mapping *"ket"*

$$\begin{array}{rcl} |x\rangle : \mathbb{C} & \to & \mathcal{X}, \\ \alpha & \mapsto & \alpha x, \end{array}$$

we can define its adjoint *"bra"* to be the unique operator $\langle x| : \mathcal{X} \to \mathbb{C}$ which satisfies $\langle x||y\rangle = \langle x, y \rangle \ \forall y \in \mathcal{X}$. We will encounter different kinds of operators throughout this thesis.

- An operator $X \in L(\mathcal{X})$ is *Hermitian* if $X^* = X$. We denote the set of such operators $\operatorname{Herm}(\mathcal{X})$.
- An operator $X \in L(\mathcal{X})$ is traceless if $\operatorname{tr}(X) = 0$. We call the set of all such operators $L_{\mathrm{tr}=0}(\mathcal{X})$
- An operator $P \in L(\mathcal{X})$ is *positive semidefinite* if it is Hermitian and all of its eigenvalues are nonnegative. The set of such operators is denoted $\operatorname{Pos}(\mathcal{X})$. We will show later on that $\operatorname{Pos}(\mathcal{X})$ represents an important convex cone in $\operatorname{Herm}(\mathcal{X})$.

- An operator $P \in L(\mathcal{X})$ is *positive definite* if it is positive semidefinite and all eigenvalues are strictly positive. The set of such operators is denoted $Pd(\mathcal{X})$. Note that all elements of $Pd(\mathcal{X})$ are invertible.
- An operator $\rho \in L(\mathcal{X})$ is a *density operator* if it is both positive semidefinite and has normalized trace: $\operatorname{tr}(\rho) = 1$. The set of such operators is denoted $D(\mathcal{X})$.
- A density operator $\rho \in D(\mathcal{X})$ is *pure* if and only if $\operatorname{tr}\left(\rho^2\right) = 1$. This is equivalent to demanding rank 1. Such operators can always be represented as $\rho = |x\rangle\langle x|$ for some $x \in \mathcal{X}$.
- An operator $U \in L(\mathcal{X})$ is *unitary,* if $U^* U = \mathbb{I}_{\mathcal{X}}$. The set of unitary operators is denoted $U(\mathcal{X})$.

For $p \in \mathbb{N}_+$ and an arbitrary operator $A \in L(\mathcal{X}, \mathcal{Y})$ the Schatten-p-norm is given by

$$\|A\|_p = \{\operatorname{tr}(|A|^p)\}^{\frac{1}{p}} . \tag{4}$$

For this thesis 3 basic operator norms are important. They are defined for any element $A \in L(\mathcal{X}, \mathcal{Y})$.

- The *trace norm* ($p = 1$): $\|A\|_1 = \operatorname{tr}(|A|)$, where $|A| = \sqrt{A^* A}$. For $X \in L(\mathcal{X})$ the following useful formula holds:

$$\|X\|_1 = \max_{U \in U(\mathcal{X})} |\langle U, X\rangle| . \tag{5}$$

- The *Hilbert-Schmidt norm* ($p = 2$): $\|A\|_2 = \sqrt{\langle A, A\rangle}$. It is sometimes also called Frobenius norm.
- The *operator norm* ($p = \infty$): $\|A\|_\infty = \max_{u \in S(\mathcal{X})} \|Au\|_2$. This norm is also denoted spectral norm.

As already mentioned, these norms correspond to the Schatten-1, the Schatten-2 and the Schatten-∞ norm and obey the following order:

$$\|A\|_\infty \leq \|A\|_2 \leq \|A\|_1 \quad \forall A \in L(\mathcal{X}, \mathcal{Y}) .$$

Further connections between these norms (duality, etc.) will be analyzed in section 2.2.

2.1.3 Measurements

A (finite dimensional) *measurement* of a quantum system on a Hilbert space $\mathcal{X}$ corresponds to a function of the form

$$\mathcal{M} : \{1, \ldots, n\} \to \operatorname{Pos}(\mathcal{X}) ,$$

where $\{1, \ldots, n\}$ is the set of measurement outcomes. We identify the measurement $\mathcal{M}$ with a collection of positive semidefinite operators $\{M_k : k \in \{1, \ldots, n\}\}$.

We call this set *POVM* (positive operator valued measure). In order to be a valid measurement, $\mathcal{M}$ has to obey

$$\sum_{k=1}^{n} M_k = \mathbb{I}_{\mathcal{X}}. \tag{6}$$

Applying a measurement to a quantum state $\rho \in D(\mathcal{X})$ implies that an element of $\{1, \ldots, n\}$ is selected randomly. The probability associated with each possible outcome $k \in \{1, \ldots, n\}$ is given by

$$p_k = \langle M_k, \rho \rangle = \operatorname{tr}(M_k \rho).$$

After the measurement, the state ρ ceases to exist. Note that (6) guarantees that $p(\rho) \in \mathbb{R}^n$ is a probability vector (i.e.: $p_i \geq 0$ for every $i \in \{1, \ldots, n\}$ and $\sum_{i=1}^{n} p_i = 1$) for any $\rho \in D(\mathcal{X})$.

A POVM-measurement $\{M_k\}_{k=1}^{n}$ is called *informationally complete* if it accesses all of $\operatorname{Herm}(\mathcal{X})$. By this we mean that for any non-vanishing ($X \neq 0$) $X \in \operatorname{Herm}(\mathcal{X})$ there exists at least one $k \in \{1, \ldots, n\}$ such that $\operatorname{tr}(M_k X) \neq 0$. In addition, we call a POVM *exactly informationally complete*, if it is informationally complete and obeys $n = \dim \operatorname{Herm}(\mathcal{X})$ (i.e the measurement is not overcomplete). SIC POVMs constitute a special family of exactly informationally complete POVMs.

2.1.4 Purifications

A useful notion concerning positive semidefinite operators is that of a *purification*. For any $P \in \operatorname{Pos}(\mathcal{X})$ and any space $\mathcal{Y}$ that satisfies $\dim(\mathcal{Y}) \geq \operatorname{rank}(P)$, a vector of the form $u \in \mathcal{X} \otimes \mathcal{Y}$ is known to exist that satisfies

$$P = \operatorname{tr}_{\mathcal{Y}}(|u\rangle\langle u|).$$

Here $\operatorname{tr}_{\mathcal{Y}}$ denotes the partial trace over $\mathcal{Y}$. Such a vector u is called a purification of P. Due to their defining property, it is necessary that any two purifications $u, v \in \mathcal{X} \otimes \mathcal{Y}$ of one operator $P \in \operatorname{Pos}(\mathcal{X})$ be unitarily equivalent. This means that there exists $U \in U(\mathcal{Y})$ such that $v = (\mathbb{I}_{\mathcal{X}} \otimes U) u$.

2.1.5 Distance measures for density operators

A density operator is the most general description of a quantum state and quantifying the distance between such operators is crucial for state discrimination. One such distance measure for two density operators $\rho, \sigma \in D(\mathcal{X})$ is given by the *trace distance*

$$\delta(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1. \tag{7}$$

It has immense operational significance. Assume that our aim is to distinguish one quantum state $\rho \in D(\mathcal{X})$ from another state $\sigma \in D(\mathcal{X})$ via an arbitrary measurement. A famous theorem by Helstrom [3] states that the probability of correctly distinguishing ρ from σ is related to $\delta(\rho,\sigma)$. In fact, the optimal bias that can be obtained corresponds to $\frac{1}{2}\delta(\rho,\sigma)$. The trace distance (7) therefore provides an upper bound on the maximal bias that is achievable via any measurement. Despite of having many nice properties, the trace norm has some disadvantageous behavior as well. In particular it is in general not stable towards purifications. Indeed, if $u,v\in\mathcal{X}\otimes\mathcal{Y}$ are purifications of $\rho,\sigma\in D(\mathcal{X})$ $(\dim(\mathcal{Y})\geq\max\{\operatorname{rank}(\rho),\operatorname{rank}(\sigma)\})$ it holds that

$$\left\||u\rangle\langle u|-|v\rangle\langle v|\right\|_1\geq\left\|\operatorname{tr}_{\mathcal{Y}}(|u\rangle\langle u|-|v\rangle\langle v|)\right\|_1=\|\rho-\sigma\|_1.$$

The inequality sign above is typically strict. This implies that purifying two systems in general amplifies their trace distance.

We now present another important distance measure that is stable towards purifications. Given two positive semidefinite operators $P,Q\in\operatorname{Pos}(\mathcal{X})$, we define the *fidelity* between them as

$$\begin{aligned} F(P,Q) &= \left\|\sqrt{P}\sqrt{Q}\right\|_1, \quad \text{or equivalently} \qquad (8)\\ F(P,Q) &= \operatorname{tr}\left(\sqrt{\sqrt{P}Q\sqrt{P}}\right). \end{aligned}$$

The fidelity is symmetric and has a particularly simple appearance if one of the states is pure:

$$F(|x\rangle\langle x|,\sigma)=\sqrt{\langle x,\sigma x\rangle}\quad\forall x\in\mathcal{X},\ \forall\sigma\in D(\mathcal{X}).$$

Note that in particular we have $F(|x\rangle\langle x|,|y\rangle\langle y|)=|\langle x,y\rangle|$ for any two pure states with $x,y\in\mathcal{X}$. Therefore the fidelity can be seen as a generalization of the quantum mechanical overlap. The fidelity is stable under the action of tensor products. For any $P_1,Q_1\in\operatorname{Pos}(\mathcal{X})$ and $P_2,Q_2\in\operatorname{Pos}(\mathcal{Y})$ the fidelity obeys

$$F(P_1\otimes Q_1,P_2\otimes Q_2)=F(P_1,Q_1)F(P_2,Q_2).$$

The following theorem underlines the stability of the fidelity towards purifications.

Uhlmann's theorem: Let $P,Q\in\operatorname{Pos}(\mathcal{X})$ and assume that both have rank at most $\dim(\mathcal{Y})$. Let $u\in\mathcal{X}\otimes\mathcal{Y}$ be any purification of P, then

$$F(P,Q)=\max\{|\langle u,v\rangle|:\ v\in\mathcal{X}\otimes\mathcal{Y},\ \operatorname{tr}_{\mathcal{Y}}(|v\rangle\langle v|)=Q\}.$$

The two distance measures (7) and (8) are related via the *Fuchs-van de Graaf inequalities*. For any $\rho,\sigma\in D(\mathcal{X})$ it holds that

$$\begin{aligned} 1-\delta(\rho,\sigma) &\leq F(\rho,\sigma)\leq\sqrt{1-\delta^2(\rho,\sigma)} \quad \text{or equivalently} \qquad (9)\\ 1-F(\rho,\sigma) &\leq \delta(\rho,\sigma)\leq\sqrt{1-F^2(\rho,\sigma)}. \qquad (10) \end{aligned}$$

The upper bound $P(\rho,\sigma):=\sqrt{1-F^2(\rho,\sigma)}$ in (10) is called purified distance and represents yet another distance measure. This metric plays a dominant role in defining smooth entropies. We refer to [12] for further information.

2.1.6 Superoperators

Linear mappings of operators are very important in quantum information in general and our work in particular. Since operators map states onto states and these mappings map operators onto operators, they are called *superoperators.* We identify $T(\mathcal{X}, \mathcal{Y})$ with the space of all linear mappings $\Phi : L(\mathcal{X}) \to L(\mathcal{Y})$. For $T(\mathcal{X}, \mathcal{X})$ we simply write $T(\mathcal{X})$. The adjoint mapping $\Phi^* \in T(\mathcal{Y}, \mathcal{X})$ of some $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is the unique mapping that obeys

$$\langle Y, \Phi(X) \rangle = \langle \Phi^*(Y), X \rangle \quad \forall X \in L(\mathcal{X}), \forall Y \in L(\mathcal{Y}).$$

We call the trivial mapping from $L(\mathcal{X})$ to itself $\mathbb{I}_{L(\mathcal{X})}$. The following classes of superoperators will be important for our work.

- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is *Hermicity-preserving* if $\Phi(\mathcal{X}) \in \mathrm{Herm}(\mathcal{Y})$ for every $X \in \mathrm{Herm}(\mathcal{X})$.
- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is *completely positive* (CP) if it holds that
$$\left(\Phi \otimes \mathbb{I}_{L(\mathcal{W})}\right)(P) \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$$
for every choice of $\mathcal{W} \simeq \mathbb{C}^k$ $(k \in \mathbb{N})$ and every $P \in \mathrm{Pos}(\mathcal{X})$.
- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is *trace-preserving* (TP) if $\mathrm{tr}(\Phi(X)) = \mathrm{tr}(X)$ for every $X \in L(\mathcal{X})$.
- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is a *quantum channel* (CPTP) if it is both completely positive and trace-preserving .
- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is an entanglement breaking channel (EB) if it is has the following form:
$$\Phi(X) = \sum_{k=1}^{n} R_k \mathrm{tr}(M_k X).$$
Here each R_k denotes a density operator and $\{M_k\}_{k=1}^n$ represents a POVM.

There are several possibilities of representing superoperators. We will restrict ourselves to two of them and refer to [11] (Lecture 5) for a more detailed survey.

The *Choi-Jamiolkowski representation* maps a superoperator $\Phi \in T(\mathcal{X}, \mathcal{Y})$ on the operator $J(\Phi) \in L(\mathcal{Y} \otimes \mathcal{X})$ defined as

$$J(\Phi) = \sum_{i,j=1}^{n} \Phi(|i\rangle\langle j|) \otimes |i\rangle\langle j|,$$

where we have assumed that $\mathcal{X} \simeq \mathbb{C}^n$ and $\mathcal{Y} \simeq \mathbb{C}^m$. The mapping J is a linear bijection from $T(\mathcal{X}, \mathcal{Y})$ to $L(\mathcal{Y} \otimes \mathcal{X})$. The operator $J(\Phi)$ therefore provides a convenient way of concretely representing superoperators as $nm \times nm$-matrices. It holds that

- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is *Hermicity-preserving* if and only if $J(\Phi)$ is Hermitian [15],

- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is *completely positive* if and only if $J(\Phi)$ is positive semidefinite [16, 17],
- $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is *trace-preserving* if and only if $\operatorname{tr}_{\mathcal{Y}}(J(\Phi)) = \mathbb{I}_{\mathcal{X}}$.

Another useful way of representing superoperators is the *Stinespring representation*. Two matrices $A, B \in L(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ are called a Stinespring pair of $\Phi \in T(\mathcal{X}, \mathcal{Y})$ if

$$\Phi(X) = \operatorname{tr}_{\mathcal{Z}}(AXB^*) \quad \forall X \in L(\mathcal{X}). \tag{11}$$

An expression of the form (11) is called a Stinespring representation of Φ. Stinespring representations are never unique and always exist for $\dim(\mathcal{Z}) \geq \operatorname{rank}(J(\Phi))$. For completely positive Φ's, one can choose Stinespring pairs that obey $A = B$. In our work we will mainly use Stinespring representations. However Choi-Jamiolkowski representations will be important for obtaining a upper (lower) bound for our sought for constants λ (μ) in subsection 4.3.4.

2.1.7 Distance measures for superoperators

In this subsection we present distance measures for arbitrary superoperators $\Phi \in T(\mathcal{X}, \mathcal{Y})$. The first quantity is the *induced 1-norm*

$$\|\Phi\|_1 = \max\{\|\Phi(X)\|_1 : \|X\|_1 \leq 1\}. \tag{12}$$

Due to the convexity of the trace norm, this expression is easily seen to be equivalent to

$$\|\Phi\|_1 = \max\{\|\Phi(|x\rangle\langle y|)\|_1 : x, y \in S(\mathcal{X})\}. \tag{13}$$

Like any induced norm, expression (12) is submultiplicative. For $\Phi \in T(\mathcal{X}, \mathcal{Y})$ and $\Psi \in T(\mathcal{Y}, \mathcal{Z})$ it holds that

$$\|\Phi\Psi\|_1 \leq \|\Phi\|_1 \|\Psi\|_1.$$

Unfortunately, the induced 1-norm is unstable (not multiplicative) with respect to Tensor products. If we, for instance, combine the transpose mapping $T \in T(\mathcal{X})$ and the identity $\mathbb{I}_{L(\mathcal{X})}$ via a tensor product, we get:

$$\left\|T \otimes \mathbb{I}_{L(\mathcal{X})}\right\|_1 \geq n > 1 = \|T\|_1 \left\|\mathbb{I}_{L(\mathcal{X})}\right\|_1$$

for any $n \geq 2$. This calls for a norm that does not admit this strange behavior. Such a distance measure is given by the *diamond norm*. For any $\Phi \in T(\mathcal{X}, \mathcal{Y})$ we write

$$\|\Phi\|_\diamond = \left\|\Phi \otimes \mathbb{I}_{L(\mathcal{X})}\right\|_1 = \max\left\{\left\|\Phi \otimes \mathbb{I}_{L(\mathcal{X})}(|u\rangle\langle v|)\right\|_1 : u, v \in S(\mathcal{X} \otimes \mathcal{X})\right\}. \tag{14}$$

Tensoring with the identity has the effect of stabilizing this norm. Indeed it can be shown that $\left\|\Phi \otimes \mathbb{I}_{L(\mathcal{Z})}\right\|_1 = \|\Phi\|_\diamond$ for any $\mathcal{Z}$ obeying $\dim(\mathcal{Z}) \geq \dim(\mathcal{X})$ and for each $\Phi_1 \in T(\mathcal{X}_1, \mathcal{Y}_1)$ and $\Phi_2 \in T(\mathcal{X}_2, \mathcal{Y}_2)$ it holds that

$$\|\Phi_1 \otimes \Phi_2\|_\diamond = \|\Phi_1\|_\diamond \|\Phi_2\|_\diamond.$$

For a proof of these properties, we refer to [11] (Lecture 21).

In subsection 2.1.5 we have introduced the trace distance (7) which gives an upper limit to state discrimination. One may consider a similar situation involving channels rather than density operators. In this framework there is an analogue of Helstrom's theorem. In this theorem the trace distance is replaced by the diamond norm. This attributes operational significance to expression (14). Finally, we mention that the diamond norm of an arbitrary super-operator can be calculated efficiently via an SDP. Such an SDP is presented in subsection 3.3.5.

The diamond norm can be seen as a stabilized generalization of the trace distance. We now introduce a fidelity based distance measure for completely positive superoperators. Let us define the *maximum output fidelity* of two CP maps $\Phi_0, \Phi_1 \in T(\mathcal{X}, \mathcal{Y})$ as

$$F_{\max}(\Phi_0, \Phi_1) = \max\left\{F\left(\Phi_0(\rho_0), \Phi_1(\rho_1)\right): \ \rho_0, \rho_1 \in D(\mathcal{X})\right\}. \tag{15}$$

This quantity can also be calculated efficiently for arbitrary CP maps. A corresponding SDP is presented in subchapter 3.3.6.

We want to conclude this subsection with an astonishing relation between (14) and (15). Let us assume that an arbitrary superoperator $\Phi \in T(\mathcal{X}, \mathcal{Y})$ is given by a Stinespring pair $A, B \in L(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$

$$\Phi(X) = \mathrm{tr}_{\mathcal{Z}}(AXB^*) \quad \forall X \in L(\mathcal{X}).$$

We define the following two channels:

$$\begin{aligned} \Psi_0(X) &:= \mathrm{tr}_{\mathcal{Y}}(AXA^*), \\ \Psi_1(X) &:= \mathrm{tr}_{\mathcal{Y}}(BXB^*). \end{aligned}$$

Then it holds that

$$\|\Phi\|_\diamond = F_{\max}(\Psi_0, \Psi_1). \tag{16}$$

For a proof of this equivalence we again refer to [11] (lecture 21). In subsection 3.3.6 we show that the maximum output fidelity can be evaluated via an SDP. Therefore (16) provides another way of efficiently calculating the diamond norm of an arbitrary superoperator $\Phi \in T(\mathcal{X}, \mathcal{Y})$.

2.2 Norms

In this section we use concepts and some notation from chapter 3. Let us consider a finite dimensional real vector space V. A *norm* $\|.\|_N$ on V is a function $\|.\|_N : V \to \mathbb{R}$ obeying the following three properties $\forall v, w \in V$:

$$\begin{aligned} \|\alpha v\|_N &= |\alpha| \, \|v\|_N \quad \forall \alpha \in \mathbb{R} \quad \text{(positive homogeneity)}, && (17) \\ \|v + w\|_N &\leq \|v\|_N + \|w\|_N \quad \text{(triangle inequality)}, && (18) \\ \|v\|_N = 0 &\Leftrightarrow v = 0 \quad \text{(non-degeneracy)}. && (19) \end{aligned}$$

Functions of this form that obey (17) and (18), but not (19) are called *seminorms.*

Every norm defines a *bounded*, *closed*, *convex*, *solid*, and *symmetric* ($K = -K$) set

$$B\left(\|.\|_N\right) = \{v \in V : \ \|v\|_N \leq 1\} \tag{20}$$

which we call the *norm ball* of $\|.\|_N$. Conversely, every closed, convex, symmetric set K induces a norm $\|.\|_K$ via

$$\|v\|_K = \inf\left\{t \geq 0 : \ tv \in K^\circ\right\}, \tag{21}$$

where K° denotes the polar[1] of K. We refer to subsection 3.1.4 for more information about polar sets. Therefore norms and convex, closed, symmetric bodies of full dimension are equivalent descriptions. Seminorms also give rise to such convex objects. On the contrary to proper norms, their "seminorm-balls" are however unbounded.

Now let W be another real vector space and $\langle ., . \rangle : \ V \times W \to \mathbb{R}$ shall denote a duality. The bipolar theorem (applied to an arbitrary norm ball K) gives rise to an important relation between *polar norms*:

$$\begin{aligned} \|w\|_K &= \max_{v \in K} \langle v, w \rangle \quad \forall w \in W, && (22) \\ \|v\|_{K^\circ} &= \max_{w \in K^\circ} \langle v, w \rangle \quad \forall v \in V. && (23) \end{aligned}$$

In principle one has to take the supremum in these formulas. However, due to the convexity of K and K°, we can safely replace it by a maximum. Formula (22) can be readily derived by starting with the induced norm description (21):

$$\begin{aligned} \|w\|_K &= \inf\left\{t \geq 0 : \ tw \in K^\circ\right\} \\ &= \inf\left\{t \geq 0 : \ \langle v, tw \rangle \leq 1 \ \forall v \in K\right\} \\ &= \inf\left\{t \geq 0 : \ \langle v, w \rangle \leq \frac{1}{t} \ \forall v \in K\right\} \\ &= \sup\left\{t \geq 0 : \ \langle v, w \rangle \leq t \ \forall v \in K\right\} \\ &= \sup_{v \in K} \langle v, w \rangle = \max_{v \in K} \langle v, w \rangle. \end{aligned}$$

Equation (23) can be derived in a similar way.

Note that if we take $V \simeq W \simeq \mathrm{Herm}\left(\mathcal{X}\right)$, $\langle X, Y \rangle = \mathrm{tr}\left(XY\right) \ \forall X, Y \in \mathrm{Herm}\left(\mathcal{X}\right)$ and $K = B\left(\|.\|_1\right)$ (the trace norm ball), formulas (22) and (23) imply the famous "duality" relation[2] between trace- and operator-norm:

$$\begin{aligned} \|X\|_1 &= \max_{\|Y\|_\infty \leq 1} \langle X, Y \rangle \quad \forall X \in \mathrm{Herm}\left(\mathcal{X}\right), \\ \|Y\|_\infty &= \max_{\|X\|_1 \leq 1} \langle X, Y \rangle \quad \forall Y \in \mathrm{Herm}\left(\mathcal{X}\right). \end{aligned}$$

[1] Actually the canonical definition is given by $\|v\|_{K^\circ} = \inf\left\{t \geq 0 : \ tx \in K\right\}$. However the bipolar theorem, which applies to (semi-) norm-balls, assures that definition (21) is equivalent to this expression.

[2] Actually this correspondence is a polarity relation, rather than a duality.

These formulas can also be proved directly by applying the spectral theorem. Since the l_2-norm ball $B\left(\|.\|_2\right)$ is self-polar, we furthermore get the following formula for complex vectors (pick $V \simeq W \simeq \mathcal{X}$, $\langle x, y\rangle = \sqrt{\sum_i \bar{x}_i y_i}$):

$$\|x\|_2 = \max_{\|y\|_2 \leq 1} \langle x, y\rangle \quad \forall x \in \mathcal{X}. \tag{24}$$

We conclude this section with a few statements about norm optimization. Norms are convex functions and norm minimization over a convex set can therefore be implemented efficiently. Norm maximization (over convex sets) on the other hand is NP-hard in general. In order to illustrate this, we consider the example maximizing the l_2-norm in $V \simeq \mathbb{R}^n$ over a convex set K. We assume without loss of generality that the convex set K is given as an affinely transformed intersection of ellipsoids, i.e.:

$$K = \left\{ x \in V : \ \frac{1}{2}\mathrm{tr}\left(X P_i\right) + \langle q_i, x\rangle + r_i \leq 0 \ \forall i = 1, \ldots, m \text{ and } Ax = b \right\}$$

with $P_i \in \mathrm{Pos}\left(\mathbb{R}^n\right)$, $q_i, \in \mathbb{R}^n$, $r_i \in \mathbb{R}$ for all $i = 1, \ldots, m$ and $A \in L\left(\mathbb{R}^n, \mathbb{R}^m\right)$ as well as $b \in \mathbb{R}^m$. An algorithm for obtaining the negative squared optimal value $(-\|x_{\mathrm{opt}}\|_2^2)$ is given by the following QCQP:

$$\begin{aligned}
&\text{minimize} && \frac{1}{2}\langle x, \left(-\mathbb{I}_V\right) x\rangle, \\
&\text{subject to} && \frac{1}{2}\langle x, P_i x\rangle + \langle q_i, x\rangle + r_i \leq 0 \quad \text{for } i = 1, \ldots m, \\
& && Ax = b.
\end{aligned}$$

This problem is a non-convex QCQP ($-\mathbb{I}_V$ is not positive semidefinite) and thus NP-hard in general.

However norm maximization is not always totally hopeless. The following theorem, for instance, states that the computational complexity of maximizing convex functions over polytopes scales linearly in the number of vertices. This implies in particular that norm maximization over sufficiently simple polytopes is indeed feasible.

Theorem Let $f: \ U \to \mathbb{R}$ be a convex function with domain $U \subseteq \mathcal{X}$ that can be efficiently evaluated for any $x \in U$. Let furthermore $K = \mathrm{conv}\left(v_1, \ldots, v_l\right)$, $K \subseteq U$ be a polytope that is characterized by l vertices $v_1, \ldots, v_l \in \mathcal{X}$. Then

$$\max_{x \in K} f\left(x\right) = \max_{1 \leq i \leq l} f\left(v_i\right).$$

Proof: The proof of this theorem is very simple. Let us pick an arbitrary element $x \in K$. Due to the definition of the convex hull (see subsection 3.1.2), we can write this x as a convex combination of extreme points:

$$x = \sum_{i=1}^{l} \alpha_i v_i \quad \text{with} \quad \sum_{i=1}^{l} \alpha_i = 1 \quad \text{and} \quad \alpha_i \geq 0 \ \forall i = 1 \ldots, l.$$

Convexity of f therefore implies

$$\begin{aligned} f(x) &= f\left(\sum_{i=1}^{l} \alpha_i v_i\right) \leq \sum_{i=1}^{l} \alpha_i f(v_i) \\ &\leq \max_{i=1,\ldots,l} f(v_i) \sum_{i=1}^{l} \alpha_i = \max_{i=1,\ldots,l} f(v_i). \qquad \square \end{aligned}$$

This theorem can also be understood geometrically. The niveau set $F := \{x \in U : f(x) \leq \max_{i=1,\ldots,l} f(v_i)\} \subseteq U$ is a convex set which contains all extreme points $v_1, \ldots, v_l$ by construction. The minimality of the convex hull thus assures $K = \operatorname{conv}\{v_1, \ldots, v_l\} \subseteq F$. Therefore $K \subseteq F$ and furthermore $K \cap F \neq \emptyset$ holds by construction as well. However, these two properties assure that the maximization of f over K indeed yields $\max_{i=1,\ldots,l} f(v_i)$.

One important consequence of this theorem is that convex maximization over the l_1-norm ball can be done efficiently in $\mathbb{R}^n$. $B(\|.\|_{l_1})$ corresponds to the n-dimensional cross polytope which is fully characterized by its $2n$ vertices:

$$B(\|.\|_{l_1}) = \operatorname{conv}\{\pm e_1, \ldots, \pm e_n\}.$$

Therefore a maximization corresponds to checking the function's value at only $2n$ points. this can be of course done efficiently.

On the contrary to this encouraging result, maximizing convex functions over other norm balls is often intractable. The l_∞-ball is a typical example for this. Maximization becomes hard, because the hypercube

$$B(\|.\|_{l_\infty}) = \{x \in \mathbb{R}^n : \quad -1 \leq x_i \leq 1 \forall i = 1, \ldots, n\}$$

possesses 2^n vertices. Therefore the above procedure requires checking a number of points that is exponential in the dimensionality of the problem.

3 Convexity

The lion's share of the work presented in this thesis belongs to the framework of convex optimization. Therefore, we devote this chapter to introducing some basic concepts of convexity. However, we restrict ourselves to presenting concepts that will later be used in our work. The basic convexity concepts are taken from [18, 19], whereas the explicit SDP realizations at the end of this chapter are due to J. Watrous [10, 11]. We refer to the first two sources for a detailed introduction into the field of convexity.

3.1 Convex sets and convex functions

In this section we introduce the basic notion of convexity. The subsections that treat properties of convex sets are strongly inspired by [18], whereas our discussion of convex functions is taken from [19].

3.1.1 Affine sets

The stage for the basic definitions of affine and convex sets is the Euclidean space $\mathbb{R}^n$. For any two points $x, y \in \mathbb{R}^n$, the line passing through both points can be parametrized in the following way:

$$l_{x,y}(\tau) = \tau x + (1 - \tau) y \quad \text{for } \tau \in \mathbb{R}. \tag{25}$$

A set $A \subseteq \mathbb{R}^n$ is an *affine set* if for arbitrary $x, y \in A$ and any $\tau \in \mathbb{R}$ we have $l_{x,y}(\tau) \in A$. In words, this definition means that an affine set contains all possible lines connecting two points of A. The idea of a line can be generalized to higher dimensions. For a finite set of points $\{x_1, \dots, x_l\} \in \mathbb{R}^n$ we call

$$x = \sum_{i=1}^{l} \alpha_i x_i \quad \text{where } \sum_{i=1}^{l} \alpha_i = 1, \quad \alpha_1, \dots, \alpha_l \in \mathbb{R}$$

an *affine combination* of $\{x_1, \dots, x_l\}$. It is easy to see that any affine set C contains all possible affine combinations of its points. The set of all affine combinations of all points from a set $A \subseteq \mathbb{R}^n$ is called the *affine hull* of A. It is denoted by $\operatorname{aff}(A)$. We note without proof that $\operatorname{aff}(A)$ is the smallest affine set that contains A: If B is any affine set containing A, then $\operatorname{aff}(A) \subseteq B$.

Affine sets can be seen as subspaces with a (possibly trivial) offset. By this we mean that we can characterize an affine set $A \subseteq \mathbb{R}^n$ via a subspace $W \subseteq \mathbb{R}^n$ and an offset vector $a \in A \subseteq \mathbb{R}^n$:

$$A = a + W = \{c + w : \ w \in W\}. \tag{26}$$

Note that, in this characterization, a can be an arbitrary element of A. For a short and elementary proof of this fact, we refer to [19]. Due to characterization (26), it makes sense to define the dimension of an affine set A as the dimension of the corresponding subspace $W = A - a$, where a can again be any element of A. We can use this affine dimension to introduce a notion of dimension for arbitrary sets: We define the affine dimension of a set $A \subseteq \mathbb{R}^n$ as the dimension of its affine hull $\operatorname{aff}(A)$.

3.1.2 Convex sets

The definition of convex sets is very similar to the definition of affine sets (25). However, rather than entire lines, only the line segment between two points is relevant. A set $K \subseteq \mathbb{R}^n$ is *convex* if $\forall x, y \in K$ and $\forall \tau \in [0, 1]$ we have

$$\tau x + (1 - \tau) y \in K. \tag{27}$$

Therefore a set is convex if and only if it contains each line segment between two arbitrary points. This implies that affine sets are also convex, whereas, conversely, any convex set K lies within the minimal affine set $\operatorname{aff}(K)$.

Similar to above, this concept can be generalized in the following way. For a finite set of points $\{x_1, \dots, x_l\} \in \mathbb{R}^n$, we call

$$x = \sum_{i=1}^{l} \alpha_i x_i \quad \text{where } \sum_{i=1}^{l} \alpha_i = 1 \quad \text{and} \quad \alpha_i \geq 0 \; \forall i = 1, \dots, l$$

a *convex combination of* $x_1, \dots, x_l$. For an arbitrary set $A \subseteq \mathbb{R}^n$, we call the set of all convex combinations of all points the *convex hull of* A. It is denoted by $\operatorname{conv}(A)$. We note without proof[3] that $\operatorname{conv}(A)$ is the smallest convex set containing A: If B is any convex set containing A, then $\operatorname{conv}(A) \subseteq B$. For the set of points $\{x_1, \dots, x_l\}$ from above we therefore have

$$\begin{aligned} \operatorname{conv}(x_1, \dots, x_l) : &= \operatorname{conv}(\{x_1, \dots, x_l\}) \\ &= \left\{ x \in \mathbb{R}^n : \; x = \sum_{i=1}^{l} \alpha_i x_i, \text{ s.t. } \sum_{i=1}^{l} \alpha_i = 1, \; \alpha_i \geq 0 \right\}. \end{aligned}$$

The idea of convex combinations can be generalized to include probability distributions (and therefore also infinite sums and integrals). However we will not require these generalizations for our work.

In the following we will present some important families of convex sets.

3.1.3 Cones

We now introduce more general concepts that are defined for arbitrary vector spaces V, rather than requiring $\mathbb{R}^n$. We call a set $C \subseteq V$ a *cone* if

$$\begin{aligned} 0 &\in C \quad \text{and} \\ \alpha x &\in C \text{ for all } \alpha \geq 0 \text{ and every } x \in C. \end{aligned}$$

A cone is *convex* if for any two points $x, y \in C$ and any $\alpha, \beta \geq 0$ we have $\alpha x + \beta y \in C$. For a finite set of points $\{x_1, \dots, x_l\} \in V$, we call

$$x = \sum_{i=1}^{l} \alpha_i x_i \quad \text{where } \alpha_i \geq 0 \; \forall i = 1, \dots, l$$

a *conic combination* of $x_1, \dots, x_l$. We call the set of all conic combinations of points from a set $A \subseteq V$ the *conic hull* of A. It shall be denoted by $\operatorname{co}(A)$. Similarly to the convex hull above, $\operatorname{co}(A)$ is the smallest convex cone that contains A.

A cone C is *pointed* if $C \cap (-C) = \{0\}$. This criterion is equivalent to demanding that C does not contain straight lines. We furthermore call a cone *solid* if it has nonempty interior. We summarize all these properties by one name:

[3] For a proof we refer to [18], Theorem 2.1.

Proper cones: A cone C is called *proper* if it is closed, convex, solid and pointed.

Let $C \subseteq V$ be a cone. A set $B \subset C$ is called a base of C if $0 \notin B$ and for any non-trivial point $u \in C$ ($u \neq 0$), there is a unique representation $u = \alpha b$ with $b \in B$ and $\alpha > 0$. We note without proof that the bases of a convex cone form convex sets and vice versa.

Any convex cone $C \subseteq V$ defines an *order* on the vector space they live in. We say that

$$\begin{aligned} x \leq_C y \qquad & \text{provided that } y - x \in C \quad \text{and} \\ x \geq_C y \qquad & \text{provided that } x - y \in C. \end{aligned}$$

However we will write $\preceq$ instead of $\leq_C$ in cases where the underlying cone is obvious. This order obeys properties that are familiar from ordinary inequalities:

- $x \geq_C x$ for any $x \in V$.
- $x \leq_C y$ and $y \leq_C z$, then $x \leq_C z$.
- If $x \leq_C y$ and $\alpha \geq 0$, then $\alpha x \leq_C \alpha y$.
- If $x_1 \leq_C y_1$ and $x_2 \leq_C y_2$, then $x_1 + x_2 \leq y_1 + y_2$.

All of these facts can be readily verified. Such orders are sometimes called generalized inequalities and properties above make this nomenclature very plausible. We give some important examples of such orders induced by a cone.

1. An order for Euclidean space $\mathbb{R}^n$: The positive orthant

   $$\mathbb{R}^n_+ = \{x \in \mathbb{R}^n : \; x_i \geq 0 \; \forall i = 1, \ldots, n\}, \tag{28}$$

   which is obviously a convex cone, induces the following generalized inequality for elements $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{R}^n$:

   $$x \preceq y \quad \Leftrightarrow \quad x_i \leq y_i \; \forall i = 1, \ldots, n.$$

2. An order for Hermitian $n \times n$ matrices $\mathrm{Herm}(\mathcal{X})$: The cone of positive semidefinite matrices

   $$\mathrm{Pos}(\mathcal{X}) = \{X \in \mathrm{Herm}(\mathcal{X}) : \; \langle x, A, x \rangle \geq 0 \; \forall x \in \mathcal{X}\} \tag{29}$$

   induces the following generalized inequality for elements A and B in $\mathrm{Herm}(\mathbb{C}^n)$:

   $$A \preceq B \quad \Leftrightarrow \quad B - A \in \mathrm{Pos}(\mathcal{X}). \tag{30}$$

   This partial order plays an important role in the field of semidefinite programming.

3. A more restrictive order for $\mathrm{Herm}(\mathcal{X})$: The set positive definite matrices

   $$\mathrm{Pd}(\mathcal{X}) = \{X \in \mathrm{Herm}(\mathcal{X}) : \; \langle x, A, x \rangle > 0 \; \forall x \in \mathcal{X}\} \tag{31}$$

   does not constitute a cone ($0 \neq \mathrm{Pd}(\mathcal{X})$) . However, it still induces the following stricter inequality for elements A and B in $\mathrm{Herm}(\mathcal{X})$:

   $$A \prec B \quad \Leftrightarrow \quad B - A \in \mathrm{Pd}(\mathcal{X}) \tag{32}$$

3.1.4 Polar sets

In order to embed the concepts of polarity and duality into a general framework, we need to introduce dualities.

Duality: Let V and W be real vector spaces. A non-degenerate bilinear form

$$\langle .,. \rangle : \; V \times W \to \mathbb{R} \tag{33}$$

is called a *duality* of V and W.

We note that this concept can be extended to topological vector spaces. However, we will not need this generalization for our work.

We now introduce the general concept of polarity assuming that we have two vector spaces V and W that are connected via a duality. Let $A \subseteq V$ be an arbitrary non-empty set. Its *polar* $A^\circ \subseteq W$ is defined to be the following set:

$$A^\circ = \left\{ y \in \mathbb{R}^n : \; \langle y, x \rangle \leq 1 \; \forall x \in A \right\}.$$

The polar can be thought of as a (non-unique) generalization of the orthogonal complement. Indeed we have for a linear subspace $L \subseteq V$

$$L^\circ = \left\{ w \in W : \; \langle v, w \rangle = 0 \; \forall v \in V \right\}.$$

In the special case $V \simeq W \simeq \mathbb{R}^n$ and $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ this is indeed the definition of the orthogonal complement $L^\perp$. In addition, the polar obeys many properties that are typical for complements:

- If $A \subseteq B$, then $B^\circ \subseteq A^\circ$.
- For a union of sets $\left\{ A_i \right\}_{i \in I}$ we have $\left(\bigcup_{i \in I} A_i \right)^\circ = \bigcap_{i \in I} A_i^\circ$.
- For any $\alpha > 0$ it holds that $(\alpha A)^\circ = \frac{1}{\alpha} A^\circ$.

All of these properties (including the next one) can be readily verified. Another interesting feature of the polar is its convexity. The polar of an arbitrary set A is a closed convex set that contains the origin. If the set A is itself already convex, the following strong statement holds in addition.

Bipolar Theorem: Let $A \subseteq \mathbb{R}^n$ be a closed convex set containing the origin. Then $(A^\circ)^\circ = A$.

For a proof of this theorem we refer to [18]. The concept of polarity is important for relating norms. We have already exploited this in section 2.2.

3.1.5 Dual cones

A concept similar to polar sets are dual sets. On the contrary to the former, dual sets are only defined for convex cones. Let $\langle .,. \rangle : \; V \times W \to \mathbb{R}$ be a duality of vector spaces and let $C \subseteq V$ be a convex cone. The cone $C^* \subseteq W$ defined via

$$C^* := \left\{ w \in W : \; \langle v, w \rangle \geq 0 \; \forall v \in C \right\}$$

is called the *dual cone of* C. Similarly, if $C \subseteq W$ is a convex cone, its dual cone $C^* \subseteq V$ is defined in an analogous way:

$$C^* = \{v \in V : \langle v, w \rangle \geq 0 \, \forall w \in C\} .$$

Similar to polar sets, dual cones are always closed, convex and contain the origin. They can also be seen as a generalization of the orthogonal complement, because for a subspace $L \subseteq V$ we again have

$$L^* = \{w \in W : \langle l, w \rangle = 0 \, \forall l \in L\} .$$

Two of the polarity properties above, as well as the Bipolar theorem, also hold for dual cones.

- If $A \subseteq B$, then $B^* \subseteq A^*$.
- For a union of sets $\{A_i\}_{i \in I}$ we have: $\left(\bigcup_{i \in I} A_i\right)^* = \bigcap_{i \in I} A_i^*$.
- "Bipolar theorem": For a proper cone C, we have $(C^*)^* = C$.

In analogy to the polar case, this underlines the interpretation of the dual as another generalization of the orthogonal complement. Cones can be their their own dual. We call such cones *self-dual.* Two prominent examples of self-dual cones are the positive orthant (28) and the cone of positive semidefinite matrices (29).

3.1.6 Polyhedra and Polytopes

A *polyhedron* P is defined to be the solution set of a finite number m of linear inequalities:

$$P = \{x \in \mathbb{R}^n : \langle c_i, x \rangle \leq \beta_i \text{ for } i = 1, \ldots, m\} . \tag{34}$$

A *polytope* Q is defined to be convex hull of a finite set of points $v_1, \ldots, v_l \in \mathbb{R}^n$:

$$Q = \operatorname{conv}(v_1, \ldots, v_l) . \tag{35}$$

Polyhedra and Polytopes are equivalent due to the following theorem.

Weyl-Minkowski Theorem: Any bounded polyhedron is a polytope and vice versa.

Therefore we shall adopt the name polytope for both objects. The Weyl-Minkowski theorem states that descriptions (34) and (35) can serve as equivalent descriptions of the same geometric object. The former characterization is called *half-space characterization*, whereas we refer to the latter as *vertex representation.* This mirrors the fact that any polytope can either be seen as an intersection of half spaces (characterization (34)) or as the convex hull of its extreme points or vertices (characterization (35)). Both representations have a very different geometric flavor and can have substantially different complexity as well. The following two examples illustrate this.

1. The cross polytope: The cross polytope or l_1-norm ball

$$B(\|.\|_1) = \{x \in \mathbb{R}^n : \|x\|_1 \leq 1\}$$

can be easily characterized via its $2n$ vertices (vertex representation):

$$B(\|.\|_1) = \operatorname{conv}(\pm e_1, \ldots, \pm e_n),$$

where e_i denotes the i-th standard basis vector. The cross polytope's (unique minimal) half space representation is given by

$$B(\|.\|_1) = \{x \in \mathbb{R}^n : \langle c, x\rangle \leq 1, \; c = (\pm 1, \ldots, \pm 1)\}. \tag{36}$$

Here the vector c actually stands for 2^n different vectors that give rise to 2^n different inequalities in the half-space representation.
For our remaining observations it is necessary to introduce some terminology. We say that a vector $\bar{x} \in \mathbb{R}^n$ *exactly* satisfies the inequality $\langle c, x\rangle \leq 1$ if $\langle c, \bar{x}\rangle = 1$. We furthermore call a set of l inequalities $\{\langle c_i, x\rangle \leq b_i\}_{i=1}^l$ *linearly independent* if the vectors $c_1, \ldots, c_l \in \mathbb{R}^n$ are linearly independent.
Note that each vertex $\pm e_i$ exactly satisfies n linear inequalities of the defining characterization[4] (36). This is no coincidence. On the contrary, a fundamental theorem [18] (Chapter II, Theorem 4.2) shows that there is a one-to-one correspondence between vertices and points that fulfill this property.
In this spirit, we define the *edges* of any polytope to be the sets that exactly satisfy $n-1$ linear independent inequalities of a defining half space characterization. It is easy to see that for bounded polyhedra these sets actually correspond line segments. In the case of the cross polytope the edges amount to the following family[5] of line segments that contains $4n(n-1)$ elements:

$$l(\tau) := \tau(\pm e_i) + (1-\tau)(\pm e_j). \tag{37}$$

Note that such an edge corresponds to a line connecting two vertices which is very intuitive. Furthermore this set of edges is already complete, because a well known result from the literature [20, 21] states that the n-dimensional cross polytope possesses exactly $4n(n-1)$ edges. The observation that these line segments exactly fulfill $(n-1)$ linear independent inequalities in (36) will become important in subsection 4.2.2.

[4] Indeed, pick for instance e_1. Then $c_1 := (1, \ldots, 1)$, $c_2 := (1, -1, 1, \ldots, 1), \ldots, c_n := (1, \ldots, 1, -1)$ denote n linearly independent vectors of the type $c = (\pm 1, \ldots, \pm 1)$ that furthermore obey $\langle c_i, e_1\rangle = 1 \; \forall i = 1, \ldots, n$. Finding n such vectors for arbitrary e_i is completely analogous.

[5] Let us focus on the special case $l_1(\tau) := \tau e_1 + (1-\tau) e_2$. Then $c_2 := (1, \ldots, 1)$, $c_3 := (1, 1, -1, 1, \ldots, 1), \ldots, c_n := (1, \ldots, 1, -1)$ constitutes a $(n-1)$-dimensional linearly independent family of vectors of the required type $c = (\pm 1, \ldots, \pm 1)$. Mentioning that $\langle l_1(\tau), c_i\rangle = \tau + (1-\tau) = 1 \; \forall \tau \in [0,1]$ allows us to conclude that l_1 is indeed an edge of $B(\|.\|_1)$. It is obvious that a similar argument holds for any other line of the type (37).

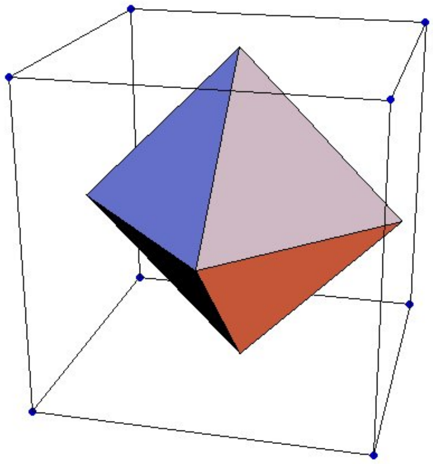


Figure 2: This graphic visualizes the unit octahedron (3D l_1-norm ball) and the unit cube (3D l_∞-norm ball) and was taken from [22]. Both objects are convex polytopes and polar to each other.

2. The hypercube: The complexity of representing the hypercube (or l_∞-norm ball)

$$B\left(\|.\|_\infty\right) = \{x \in \mathbb{R}^n : \ 0 \leq x_i \leq 1 \ \forall i = 1, \ldots, n\}$$

behaves exactly the other way round. Its vertex representation requires all 2^n extreme points, whereas its half-space characterization is given by the following $2n$ linear inequalities:

$$\begin{array}{rcl} \langle e_1, x \rangle & \leq & 1, \\ \langle -e_1, x \rangle & \leq & 1, \\ & \vdots & \\ \langle e_n, x \rangle & \leq & 1, \\ \langle -e_n, x \rangle & \leq & 1. \end{array}$$

Hence, compared to the cross polytope, the complexity of the two representations is reversed (2^n versus $2n$).

Note that the hypercube and the cross polytope are polar to each other in any dimension. The 3 dimensional versions of the cross polytope and the hypercube are depicted in figure 2. We conclude this subsection by stating the obvious fact that both polytopes have full affine dimension n.

3.2 Convex functions

3.2.1 Definition of convex functions

Let us consider an arbitrary vector space V. A function $f : U \to \mathbb{R}$, where $U \subseteq V$ is the functions domain, is *convex* if U is a convex set and $\forall x, y \in U$ and $\tau \in [0,1]$ we have

$$f\left(\tau x + (1-\tau) y\right) \leq \tau f(x) + (1-\tau) f(y). \tag{38}$$

A function f is called *strictly convex* if strict inequality holds in (38). We say that a function f is *concave* if $(-f)$ is convex, and f is *strictly concave* if $(-f)$ is strictly convex.

The following criterion for convexity is taken from [19] and very useful.

> A function is convex if and only if it is convex when restricted to any line that intersects its domain.

Convex functions are always continuous on the relative interior of their domain. For the vector space $V \simeq \mathbb{C}^n$ analytical formulas for determining convexity do exist for differentiable functions. Although we will hardly ever use them, we state two of them for the sake of completeness.

1. First-order conditions: A differentiable function $f : U \to \mathbb{R}$ with domain $U \subseteq \mathbb{C}^n$ is convex if and only if U is a convex set and

   $$f(y) \geq f(x) + \langle \nabla f(x), y - x \rangle \quad \forall x, y \in U, \tag{39}$$

   where $\langle .,. \rangle$ denotes the standard scalar product of $\mathbb{C}^n$.
   Note that the affine function on the right hand side of (39) denotes the first order Taylor expansion of f.

2. Second-order conditions: A twice differentiable function $f : U \to \mathbb{R}$ with domain $U \subseteq \mathbb{C}^n$ is convex if and only if U is convex and

   $$\triangle f(x) \succeq 0, \tag{40}$$

   where $\triangle f(x) \in L(\mathbb{C}^n)$ denotes the Hesse matrix in x and $\succeq$ corresponds to the usual partial order $\geq_{\mathrm{Pos}(\mathbb{C}^n)}$.

Note that criterion one implies that the first order Taylor expansion of a convex function is a global underestimator. This allows us to obtain global information (a global underestimator) from local information $(f(x) + \langle \nabla f(x), y - x \rangle$ at a certain point $x \in U)$. Furthermore, (39) implies that a convex function has a single global minimum at $x_0 \in U$ obeying $\nabla f(x_0) = 0$. These two properties also apply to non-differentiable convex functions and are very useful for convex minimization.

3.2.2 Affine transformations

Affine transformations are one particularly important family of convex functions. Recall that we have identified affine sets A with a vector space and an offset. In the same spirit we define affine functions f to be linear functions with an offset, i.e.:

$$f(x) = Ax + b, \tag{41}$$

where $A: V \to W$ is a linear transformation between vector spaces and $b \in W$ is an offset. It can be easily seen that affine transformations preserve straight lines. This implies that they also *preserve convexity*. Consequently, affine transformations are convex as well as concave functions.

3.3 Convex optimization

3.3.1 Convex Optimization

Convex optimization studies the problem of minimizing convex functions over convex sets. This objective is equivalent to maximizing concave functions[6] over convex sets. Due to the "nice" properties of convex functions, this kind of optimization is "easier" than a general one. For instance, we have already pointed out in subsection 3.2.1 that convex functions allow for obtaining a global underestimator from local information alone. Convexity furthermore guarantees that any local minimum is also a global one. Among others, these two properties allow for tracking convex optimization problems computationally efficiently.

We now state convex optimization in its most general form. Let U be a convex subset of a real vector space V and let $f: U \to \mathbb{R}$ be a convex function. We then want to find $x_{\min} \in U$ such that

$$f(x_{\min}) = \min \{ f(x) : x \in U \}.$$

Alternatively, we can reformulate this aim in the following way:

$$\begin{array}{ll} \text{minimize} & f(x) \\ \text{subject to} & g_i(x) \leq 0 \quad \text{for } i = 1, \ldots, m. \end{array}$$

Here $g_i: V \to \mathbb{R}$ are convex functions that define U in the sense that $U = \bigcap_{i=1}^{m} \{x \in V : g_i(x) \leq 0\}$.

Many contemporary methods allow for solving such convex optimization problems efficiently. We refer to [19] for further information. In the next subchapter we introduce a particularly important subfamily of convex optimization problems: linear programming.

[6] Replacing a concave objective function f by $(-f)$ – which is convex – and consequently rendering maximization to minimization yields an equivalent convex minimization problem.

3.3.2 General Linear Programming

Linear programming can be seen as the theory of general linear inequalities and thus extends linear algebra. As we have seen in subsection 3.1.3, general linear inequalities are induced by convex cones. Therefore this general theory is sometimes called "conic linear programming". We now introduce Barvinok's general framework of linear programming [18]. Let

$$\begin{aligned} \langle .,. \rangle_1 :\; V_1 \times W_1 &\rightarrow \mathbb{R} \quad \text{and} \\ \langle .,. \rangle_2 :\; V_2 \times W_2 &\rightarrow \mathbb{R} \end{aligned}$$

be dualities connecting the vector spaces V_1 and W_1 as well as V_2 and W_2. We furthermore fix convex cones $K_1 \subseteq V_1$ and $K_2 \subseteq V_2$. By duality, these cones give rise to dual cones $K_1^* \subseteq W_1$ and $K_2^* \subseteq W_2$. Let now

$$\Phi :\; V_1 \rightarrow V_2$$

be a linear transformation, and let

$$\Phi^* :\; W_2 \rightarrow W_1$$

denote its dual transformation, i.e:

$$\langle \Phi(x), y \rangle_2 = \langle x, \Phi^*(y) \rangle_1 \quad \forall x \in V_1,\ \forall y \in W_2. \tag{42}$$

Finally, we pick some $a \in V_1$ and $b \in V_2$. Now we are ready to state the general form of a pair of linear programming problems.

Primal Problem:

$$\begin{array}{rl} \text{Find} & \gamma = \inf \langle x, a \rangle_1 \\ \text{subject to} & \Phi(x) \geq_{K_2} b, \\ & x \geq_{K_1} 0. \end{array}$$

Dual Problem:

$$\begin{array}{rl} \text{Find} & \beta = \sup \langle b, y \rangle_2 \\ \text{subject to} & \Phi^*(y) \leq_{K_1^*} a, \\ & y \geq_{K_2^*} 0. \end{array}$$

We call a point $x \in V_1$ *primal feasible* if it satisfies the required conditions $\Phi(x) \geq_{K_2} b$ and $x \geq_{K_1} 0$. Similarly we call a point $y \in W_2$ *dual feasible* if it satisfies the required conditions $\Phi^*(y) \leq_{K_1^*} a$ and $y \geq_{K_2^*} 0$. As a refinement, we call a point $x \in V_1$ ($x \in V_2$) *strictly primal feasible* (*strictly dual feasible*) if the required inequalities hold strictly. We agree on setting $\gamma = +\infty$ if there is no primal feasible plan, whereas we set $\beta = -\infty$ if there is no dual feasible y. We furthermore call x (or y) *optimal* if the infimum γ (supremum β) is attained at that point. The following theorem induces an order between any primal and dual optimal solutions.

Theorem (Weak Duality): For any primal feasible $x \in V_1$ and any dual feasible $y \in W_2$ we have

$$\langle x, a \rangle_1 \leq \langle b, y \rangle_2. \tag{43}$$

Proof: Since $x \in V_1$ is primal feasible and $y \in W_2$ is dual feasible, we get the following properties from the constraints:

$$\begin{array}{rcl} \Phi(x) - b & \in & K_2, \\ x & \in & K_1, \\ a - \Phi^*(y) & \in & K_1^*, \\ y & \in & K_2^*. \end{array}$$

Combining the second and the third element via $\langle ., . \rangle_1$ yields

$$0 \leq \langle x, a - \Phi^*(y) \rangle_1 \Rightarrow \langle x, a \rangle_1 \geq \langle x, \Phi^*(y) \rangle_1. \tag{44}$$

due to the defining relation between K_1 and its dual K_1^*. We can combine the first and fourth elements via $\langle ., . \rangle_2$ in a similar way:

$$0 \leq \langle \Phi(x) - b, y \rangle_2 \Rightarrow \langle \Phi(x), y \rangle_2 \geq \langle b, y \rangle_2, \tag{45}$$

We conclude the proof by combining inequalities (44) and (45) via the defining property (42) of Φ^*:

$$\langle b, y \rangle_2 \leq \langle \Phi(x), y \rangle_2 = \langle x, \Phi^*(y) \rangle_1 \leq \langle x, a \rangle_1. \qquad \square \tag{46}$$

The theorem states that any primal objective value $\langle x, a \rangle_1$ is always an upper bound for every possible dual objective value $\langle b, y \rangle_2$. In particular this is also true for the optimal values:

$$\beta \leq \gamma. \tag{47}$$

A particularly interesting situation occurs if this duality gap (47) vanishes, i.e. if

$$\beta = \gamma \quad \text{(strong duality)}. \tag{48}$$

Condition (48) is called *strong duality* and, if it holds, primal and dual problem are equivalent. This situation is actually quite common and many sufficient criteria for it to hold are known. We can extract one such criterion from the inequality chain (46).

Corollary (Compelementary Slackness): Suppose that $x \in V_1$ is a primal feasible plan and $y \in W_2$ is a dual feasible plan. Then both x and y are optimal and strong duality holds ($\langle b, y \rangle_2 = \beta = \gamma = \langle x, a \rangle_1$) if and only if

$$\langle x, a - \Phi^*(y) \rangle_1 = 0 \quad \text{and} \quad \langle \Phi(x) - b, y \rangle_2 = 0. \tag{49}$$

Proof: Strong duality for optimal values x and y renders the inequality chain (46) to an equality:

$$\beta = \langle b, y \rangle_2 = \langle \Phi x, y \rangle_2 = \langle x, \Phi^* y \rangle_1 = \langle x, a \rangle_1 = \gamma.$$

From this we can immediately deduce (49). In order to show the other direction, we note that condition (49) also enforces equality in (46), since it implies $\langle \Phi(x), y\rangle_2 = \langle b, y\rangle_2$ as well as $\langle x, a\rangle_1 = \langle x, \Phi^*(y)\rangle_1$. We therefore get $\langle x, a\rangle_1 = \langle b, y\rangle_2$. Combining this with the trivial inequalities $\langle b, y\rangle_2 \leq \beta$ and $\langle x, a\rangle_1 \geq \gamma$ yields

$$\beta \geq \langle b, y\rangle_2 = \langle x, a\rangle_1 \geq \gamma.$$

This however is just the converse of weak duality (47). Combining both implies strong duality ($\beta = \gamma$). □

In the following chapter we will introduce an important explicit realization of these rather abstract concepts.

3.3.3 Semidefinite Programming

Semidefinite Programming (SDP) is an explicit realization of linear programming for Hermitian matrices. We set $V_1 \simeq W_1 \simeq \mathrm{Herm}(\mathbb{C}^n)$ and $V_2 \simeq W_2 \simeq \mathrm{Herm}(\mathbb{C}^m)$ for some $n, m \in \mathbb{N}$. We consider the dualities to be the usual Hilbert-Schmidt products on $\mathrm{Herm}(\mathbb{C}^n)$ and $\mathrm{Herm}(\mathbb{C}^m)$, respectively:

$$\begin{aligned} \langle ., .\rangle_1 : \mathrm{Herm}(\mathbb{C}^n) \times \mathrm{Herm}(\mathbb{C}^n) &\rightarrow \mathbb{R}, \\ (X_1, Y_1) &\mapsto \mathrm{tr}(X_1 Y_1), \\ \langle ., .\rangle_2 : \mathrm{Herm}(\mathbb{C}^m) \times \mathrm{Herm}(\mathbb{C}^m) &\rightarrow \mathbb{R}, \\ (X_2, Y_2) &\mapsto \mathrm{tr}(X_2 Y_2). \end{aligned}$$

We pick the following asymmetric cones:

$$\begin{aligned} K_1 &:= \mathrm{Pos}(\mathbb{C}^n) \subseteq \mathrm{Herm}(\mathbb{C}^n), \\ K_2 &:= \{0\}. \end{aligned}$$

The cone K_1 induces the usual ordering on $\mathrm{Herm}(\mathbb{C}^n)$ which we shall denote by "$\preceq$". In particular $X \succeq 0$ is equivalent to $X \in \mathrm{Pos}(\mathbb{C}^n)$. The second cone gives rise to a a very restrictive order on $\mathrm{Herm}(\mathbb{C})^m$, namely $X \leq_{K_2} Y$ if and only if $X = Y \; \forall X, Y \in \mathrm{Herm}(\mathbb{C}^m)$. It thus makes sense to replace "$\leq_{K_2}$" by "$=$". The dual cones amount to

$$\begin{aligned} K_1^* &= K_1 = \mathrm{Pos}(\mathbb{C}^n) \quad \text{and} \\ K_2^* &= \mathrm{Herm}(\mathbb{C}^m). \end{aligned}$$

The cone $K_2^* = \mathrm{Herm}(\mathbb{C}^m)$ induces a trivial ordering, namely $X \leq_{K_2} Y$ for any pair $X, Y \in \mathrm{Herm}(\mathbb{C}^m)$. In particular the condition $Y \geq_{K_2^*} 0$ is equivalent to $Y \in \mathrm{Herm}(\mathbb{C}^m)$.

With these choices, any pair of semidefinite programs is completely specified by a triple (Φ, A, B):

$$\begin{aligned} \Phi : \mathrm{Herm}(\mathbb{C}^n) &\rightarrow \mathrm{Herm}(\mathbb{C}^m), \\ A &\in \mathrm{Herm}(\mathbb{C}^n), \\ B &\in \mathrm{Herm}(\mathbb{C}^m). \end{aligned}$$

Here A and B are matrices and Φ is a hermicity preserving linear mapping. We are now ready to state the linear problems for this special case:

$$\begin{array}{rl} \text{Primal Problem} & \text{Dual Problem} \\ \text{Find} \quad \gamma = \inf \langle X, A \rangle_1, & \text{Find} \quad \beta = \sup \langle B, Y \rangle_2, \\ \text{subject to:} \quad \Phi(X) = B, & \text{subject to:} \quad \Phi^*(Y) \preceq A, \\ X \in \operatorname{Pos}(\mathbb{C}^n). & Y \in \operatorname{Herm}(\mathbb{C}^m). \end{array}$$

Note that weak duality ($\beta \leq \gamma$) surely holds for these programs. Finally we replace A by $(-A)$ and Y by $(-Y)$ to bring these programs into Watrous' [11] standard form.

Primal Problem:

$$\begin{array}{rl} \text{maximize} & \langle X, A \rangle \\ \text{subject to} & \Phi(X) = B \\ & X \in \operatorname{Pos}(\mathbb{C}^n). \end{array} \tag{50}$$

Dual Problem:

$$\begin{array}{rl} \text{minimize} & \langle B, Y \rangle \\ \text{subject to} & \Phi^*(Y) \succeq A, \\ & Y \in \operatorname{Herm}(\mathbb{C}^m). \end{array} \tag{51}$$

Note that our change of variables ($A \mapsto -A$ and $Y \mapsto -Y$) also flips around weak duality:

$$\gamma = \max \langle X, A \rangle \leq \min \langle B, Y \rangle = \beta.$$

Unlike weak duality, complementary slackness directly translates into this altered framework, because the two additional minus-signs exactly compensate each other.

A highly valuable feature of semidefinite programming is that it usually obeys strong duality. The following theorem provides a powerful sufficient criterion for this situation.

Theorem (Slater's Theorem) The following implications hold for every SDP (Φ, A, B) of the above form.

1. If the primal problem is feasible and there exists a strictly feasible $Y \in \operatorname{Herm}(\mathbb{C}^m)$, then strong duality holds and the primal maximum is acquired for some $X \in \operatorname{Herm}(\mathbb{C}^n)$.
2. If the dual problem is feasible and there exists a strictly feasible $X \in \operatorname{Herm}(\mathbb{C}^n)$, then strong duality holds and the dual maximum is acquired for some $Y \in \operatorname{Herm}(\mathbb{C}^m)$.

We refer to [11] for a proof of this important theorem.

In the following subsection we present and analyze some SDPs that will be important in the remainder of our work.

3.3.4 An SDP for the trace norm

The basic expression for the trace norm $\|M\|_1$ of an arbitrary Hermitian matrix $M \in \mathrm{Herm}\left(\mathbb{C}^n\right)$ can be rewritten in the following way:

$$\|M\|_1 = \mathrm{tr}\left(|M|\right) = \mathrm{tr}\left(P_+ M\right) - \mathrm{tr}\left(P_- M\right),$$

where P_+ is the orthogonal projector onto the non-negative eigenspace of M (i.e. $P_+ M P_+ \succeq 0$) and P_- is the projector onto the negative eigenspace (i.e. $P_- M P_- \prec 0$). These projectors are complementary in the sense that they obey

$$\begin{aligned} P_+ + P_- &= \mathbb{I}_{n\times n}, \\ P_+, P_- &\in \mathrm{Pos}\left(\mathbb{C}^n\right). \end{aligned}$$

This can be seen by considering a spectral decomposition $M = \sum_{i=1}^n \mu_i |i\rangle\langle i|$ of our matrix of interest. Then $P_+ = \sum_{\mu_i \geq 0} |i\rangle\langle i|$, $P_- = \sum_{\mu_i < 0} |i\rangle\langle i|$ and the right hand side of the above equation really equals the trace norm of M:

$$\mathrm{tr}\left(P_+ M\right) - \mathrm{tr}\left(P_- M\right) = \sum_{\mu_i \geq 0} \mu_i - \sum_{\mu_i < 0} \mu_i = \sum_{i=1}^n |\mu_i| = \mathrm{tr}\left(|M|\right).$$

It is obvious that this grouping of eigenvalues is optimal and that for all other complementary projectors P and Q the expression $\mathrm{tr}\left(PM\right) - \mathrm{tr}\left(QM\right)$ is smaller. This insight tells us that $\|M\|_1$ can be found by running the following program:

$$\begin{aligned} \text{maximize} \quad & \mathrm{tr}\left(PM\right) - \mathrm{tr}\left(QM\right) \\ \text{subject to} \quad & P + Q = \mathbb{I}_{n\times n}, \\ & P, Q \in \mathrm{Pos}\left(\mathbb{C}^n\right). \end{aligned} \tag{52}$$

This program however is an SDP. Indeed the following choice of variables and parameters reduces the standard primal SDP form (50) to (52):

$$\begin{aligned} X &= \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix} \in \mathrm{Herm}\left(\mathbb{C}^n \oplus \mathbb{C}^n\right), \\ A &= \begin{pmatrix} M & 0 \\ 0 & -M \end{pmatrix} \in \mathrm{Herm}\left(\mathbb{C}^n \oplus \mathbb{C}^n\right), \\ B &= \mathbb{I}_{n\times n} \in \mathrm{Herm}\left(\mathbb{C}^n\right), \\ \Phi: & \quad \mathrm{Herm}\left(\mathbb{C}^n \oplus \mathbb{C}^n\right) \to \mathrm{Herm}\left(\mathbb{C}^n\right), \\ & \quad X = \begin{pmatrix} P & \cdot \\ \cdot & Q \end{pmatrix} \mapsto P + Q, \\ \Phi^*: & \quad \mathrm{Herm}\left(\mathbb{C}^n\right) \to \mathrm{Herm}\left(\mathbb{C}^n \oplus \mathbb{C}^n\right), \\ & \quad Y \mapsto \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix}. \end{aligned}$$

Here the dots "." in $\begin{pmatrix} P & \cdot \\ \cdot & Q \end{pmatrix}$ indicate that we do not care about the off-diagonal entries. Note that Φ^* really is the adjoint of Φ, because for any $X =$

$\begin{pmatrix} P & \cdot \\ \cdot & Q \end{pmatrix}$ and Y we have:

$$\begin{aligned}\langle \Phi\left(X\right), Y\rangle &= \langle P+Q, Y\rangle = \langle P, Y\rangle + \langle Q, Y\rangle \\ &= \left\langle \begin{pmatrix} P & \cdot \\ \cdot & Q \end{pmatrix}, \begin{pmatrix} Y & 0 \\ 0 & Y \end{pmatrix} \right\rangle = \langle X, \Phi^*\left(Y\right)\rangle.\end{aligned}$$

Using this adjoint, we can directly state the corresponding dual problem:

$$\begin{aligned} \text{minimize} \quad & \operatorname{tr}\left(Y\right), \\ \text{subject to} \quad & Y \succeq M \text{ and } Y \succeq -M, \\ & Y \in \operatorname{Herm}\left(\mathbb{C}^n\right). \end{aligned} \tag{53}$$

It is easy to see that this minimization also yields $\|M\|_1$. Therefore strong duality holds. This observation is consistent with Slater's theorem which is fulfilled, because $X = \begin{pmatrix} \mathbb{I}_{n\times n} & 0 \\ 0 & 0 \end{pmatrix}$ is a primal feasible point and $|M| + \mathbb{I}$ is strictly dual feasible.

This SDP can be efficiently implemented and guarantees that the trace norm of an arbitrary matrix can be efficiently calculated.

3.3.5 An SDP for the diamond norm squared

In this subsection we present an SDP for the diamond norm of an arbitrary superoperator Φ. It is due to J. Watrous [10, 11]. We assume that the superoperator of interest is given by a Stinespring representation

$$\begin{aligned} \Phi: \ L\left(\mathcal{X}\right) &\rightarrow L\left(\mathcal{Y}\right), \\ X &\mapsto \operatorname{tr}_{\mathcal{Z}}\left(A_0 X A_1^*\right), \end{aligned}$$

for a pair of linear transformations $A_0, A_1 : \ L\left(\mathcal{X}\right) \rightarrow L\left(\mathcal{Y}\otimes\mathcal{Z}\right)$. The pair of SDP's amounts to the following two expressions.

Primal problem:

$$\begin{aligned} \text{maximize} \quad & \langle A_1 A_1^*, X\rangle, \\ \text{subject to} \quad & \operatorname{tr}_{\mathcal{Y}}\left(X\right) = \operatorname{tr}_{\mathcal{Y}}\left(A_0 \rho A_0^*\right), \\ & \rho \in D\left(\mathcal{X}\right), \\ & X \in \operatorname{Pos}\left(\mathcal{Y}\otimes\mathcal{Z}\right). \end{aligned}$$

Dual problem:

$$\begin{aligned} \text{minimize} \quad & \left\|A_0^*\left(\mathbb{I}_{\mathcal{Y}}\otimes Y\right)A_0\right\|_\infty, \\ \text{subject to} \quad & \mathbb{I}_{\mathcal{Y}}\otimes Y \geq A_1 A_1^*, \\ & Y \in \operatorname{Pos}\left(\mathcal{Z}\right). \end{aligned}$$

These two problems indeed descend from an SDP in standard form that contains the triple (A, B, Ξ) and a primal variable $\tilde{X}$ as well as a dual variable $\tilde{Y}$:

$$
\begin{array}{rcl}
\tilde{X} & = & \begin{pmatrix} X & . \\ . & \rho \end{pmatrix} \in \operatorname{Herm}\left([\mathcal{Y} \otimes \mathcal{Z}] \oplus \mathcal{X}\right), \\
\tilde{Y} & = & \begin{pmatrix} \lambda & 0 \\ 0 & Y \end{pmatrix} \in \operatorname{Herm}\left(\mathbb{C} \oplus \mathcal{Z}\right), \\
A & = & \begin{pmatrix} A_1 A_1^* & 0 \\ 0 & 0 \end{pmatrix} \in \operatorname{Herm}\left([\mathcal{Y} \otimes \mathcal{Z}] \oplus \mathcal{X}\right), \\
B & = & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \operatorname{Herm}\left(\mathbb{C} \oplus \mathcal{Z}\right), \\
\Xi : & & \operatorname{Herm}\left([\mathcal{Y} \otimes \mathcal{Z}] \oplus \mathcal{X}\right) \to \operatorname{Herm}\left(\mathbb{C} \oplus \mathcal{Z}\right), \\
 & & Z = \begin{pmatrix} X & . \\ . & \rho \end{pmatrix} \mapsto \begin{pmatrix} \operatorname{tr}(\rho) & 0 \\ 0 & \operatorname{tr}_{\mathcal{Y}}(X) - \operatorname{tr}_{\mathcal{Y}}\left(A_0 \rho A_0^*\right) \end{pmatrix}, \\
\Xi^{*}: & & \operatorname{Herm}\left(\mathbb{C} \oplus \mathcal{Z}\right) \to \operatorname{Herm}\left([\mathcal{Y} \otimes \mathcal{Z}] \oplus \mathcal{X}\right), \\
 & & Y = \begin{pmatrix} \lambda & 0 \\ 0 & Y \end{pmatrix} \mapsto \begin{pmatrix} \mathbb{I}_{\mathcal{Y}} \otimes Y & 0 \\ 0 & \lambda \mathbb{I}_{\mathcal{X}} - A_0^* \left(\mathbb{I}_{\mathcal{Y}} \otimes Y\right) A_0 \end{pmatrix}.
\end{array}
$$

We point out that Ξ and Ξ^* are indeed dual to each other. However we abdicate showing this explicitly. Furthermore strong duality holds due to Slater's theorem, because $\tilde{Y}$ with $\lambda = (\|A_1 A_1^*\| \, \|A_0 A_0^*\| + 1)$ and $Y = (\|A_1 A_1^*\| + 1) \, \mathbb{I}_{\mathcal{Z}}$ is strictly dual feasible. The primal problem is of course feasible, because we can choose $\rho \in D(\mathcal{X})$ arbitrary and set $X = A_0 \rho A_0^*$.

For this semidefinite program the optimal solution $\alpha = \beta$ is equal to $\|\Phi\|_{\diamond}^2$. For a proof of this equality we refer to [10].

3.3.6 An SDP for the maximum output fidelity

Recall the maximum output fidelity of two completely positive superoperators $\Phi_0, \Phi_1 : \; L(\mathcal{X}) \to L(\mathcal{Z})$:

$$
F_{\max}\left(\Phi_0, \Phi_1\right) = \max\left\{F\left(\Psi_0\left(\rho_0\right), \Psi_1\left(\rho_1\right)\right) : \; \rho_0, \rho_1 \in D(\mathcal{X})\right\}.
$$

This is the maximum fidelity that can exist between any two outputs of the different mappings. We assume that the two superoperators are given via Stinespring representations:

$$
\begin{array}{rcl}
\Psi_0(X) & = & \operatorname{tr}_{\mathcal{Y}}\left(A_0 X A_1^*\right), \\
\Psi_1(X) & = & \operatorname{tr}_{\mathcal{Y}}\left(B_0 X B_1^*\right),
\end{array}
$$

for linear transformations $A_i, B_i : \; \mathcal{X} \to \mathcal{Y} \otimes \mathcal{Z}$. Note that these superoperators admit the following dual representation:

$$
\begin{array}{rcl}
\Psi_0^*, \Psi_1^* : \; L(\mathcal{Z}) & \to & L(\mathcal{X}), \\
\Psi_0^*(Z) & = & A_0^*\left(Z \otimes \mathbb{I}_{\mathcal{Y}}\right) A_1, \\
\Psi_1^*(Z) & = & B_0^*\left(Z \otimes \mathbb{I}_{\mathcal{Y}}\right) B_1.
\end{array}
$$

Indeed, Ψ_0^* obeys its defining property (42):

$$\begin{aligned} \langle \Psi_0(\rho_0), Z\rangle &= \langle \mathrm{tr}_{\mathcal{Y}}(A_0\rho_0 A_1^*), Z\rangle = \langle A_0\rho_0 A_1^*, \mathbb{I}_{\mathcal{Y}} \otimes Z\rangle \\ &= \langle \rho_0, A_0^*(\mathbb{I}_{\mathcal{Y}} \otimes Z) A_1^*\rangle = \langle \rho_0, \Psi_0^*(Z)\rangle . \end{aligned}$$

Showing that the same is true for Ψ_1^* is completely analogous. The maximum output fidelity can be calculated via the following SDP which is again due to J. Watrous [11] (chapter 21):

Primal problem :

$$\begin{aligned} \text{maximize} \quad & \frac{1}{2}\mathrm{tr}(Y) + \frac{1}{2}\mathrm{tr}(Y^*), \\ \text{subject to} \quad & \begin{pmatrix} \Psi_0(\rho_0) & Y \\ Y^* & \Psi_1(\rho_1) \end{pmatrix} \geq 0, \\ & \rho_0, \rho_1 \in D(\mathcal{X}), \\ & Y \in \mathrm{Herm}(\mathcal{Z}). \end{aligned}$$

Dual problem:

$$\begin{aligned} \text{minimize} \quad & \frac{1}{2}\left\|\Psi_0^*(Z_0)\right\|_\infty + \frac{1}{2}\left\|\Psi_1^*(Z_1)\right\|_\infty, \\ \text{subject to} \quad & \begin{pmatrix} Z_0 & -\mathbb{I}_{\mathcal{Z}} \\ \mathbb{I}_{\mathcal{Z}} & Z_1 \end{pmatrix} \geq 0, \\ & Z_0, Z_1 \in \mathrm{Pos}(\mathcal{X}). \end{aligned}$$

Note that strong duality holds here due to Slater's theorem[7]. The point $Y = 0$ is primal feasible, whereas the point characterized by $Z_0 = Z_1 = 2\mathbb{I}$ is strictly dual feasible. This SDP actually descends from a standard form SDP containing a triple (Ξ, A, B), a primal variable $\tilde{Y}$ and a dual variable $\tilde{Z}$. We summarized this standard form SDP in table 1. Again, we will not show explicitly that this SDP can actually be reduced to the simple form above. For a verification of the fact that the above problem really yields the maximum output fidelity, we refer to [11].

This fidelity notion is particularly significant, since it can serve to calculate the diamond norm of an arbitrary superoperator - see subsection 2.1.7, formula (16).

We furthermore point out that we can without difficulty restrict this SDP to the case where $\rho := \rho_0 = \rho_1$ is fixed. This allows us to calculate the fidelity of specific superoperator outputs

$$F(\Phi_0(\rho), \Phi_1(\rho)) \quad \text{for any } \rho \in D(\mathcal{X}) \tag{54}$$

via an SDP. We will use this in section 4.3.4.

[7] Actually Slater's theorem can only be applied to the standard SDP presented below. However the following feasible points can straightforwardly be embedded into the standard form by adjusting the additional parameters accordingly.

$$\begin{aligned}
\tilde{Y} &= \begin{pmatrix} P & Y & & . \\ Y^* & Q & & \\ & & \rho_0 & . \\ . & & . & \rho_1 \end{pmatrix} \in \mathrm{Herm}\left(\mathcal{Z}^2 \oplus \mathcal{X}^2\right), \\
\tilde{Z} &= \begin{pmatrix} Z_0 & . & & . \\ . & Z_1 & & \\ & & \lambda_1 & . \\ . & & . & \lambda_2 \end{pmatrix} \in \mathrm{Herm}\left(\mathcal{Z}^2 \oplus \mathbb{C}^2\right), \\
A &= \frac{1}{2}\begin{pmatrix} 0 & \mathbb{I}_{\mathcal{Z}} & & 0 \\ \mathbb{I}_{\mathcal{Z}} & 0 & & \\ & & 0 & \\ 0 & & & 0 \end{pmatrix} \in \mathrm{Herm}\left(\mathcal{Z}^2 \oplus \mathcal{X}^2\right), \\
B &= \begin{pmatrix} 0 & 0 & & 0 \\ 0 & 0 & & \\ & & 1 & 0 \\ 0 & & 0 & 1 \end{pmatrix} \in \mathrm{Herm}\left(\mathcal{Z}^2 \oplus \mathbb{C}^2\right), \\
\Xi: \quad & L\left(\mathcal{Z}^2 \oplus \mathcal{X}^2\right) \to L\left(\mathcal{Z}^2 \oplus \mathbb{C}^2\right) \\
& \tilde{Y} = \begin{pmatrix} P & Y & & . \\ Y^* & Q & & \\ & & \rho_0 & . \\ . & & . & \rho_1 \end{pmatrix} \mapsto \begin{pmatrix} P - \Psi_0\left(\rho_0\right) & 0 & & 0 \\ 0 & Q - \Psi_1\left(\rho_1\right) & & \\ & & \mathrm{tr}\left(\rho_0\right) & 0 \\ 0 & & 0 & \mathrm{tr}\left(\rho_1\right) \end{pmatrix}, \\
\Xi^*: \quad & L\left(\mathcal{X}^2 \oplus \mathbb{C}^2\right) \to L\left(\mathcal{Z}^2 \oplus \mathcal{X}^2\right), \\
& \tilde{Z} = \begin{pmatrix} Z_0 & . & & . \\ . & Z_1 & & \\ & & \lambda_1 & . \\ . & & . & \lambda_2 \end{pmatrix} \mapsto \begin{pmatrix} Z_0 & 0 & & 0 \\ 0 & Z_1 & & \\ & & \lambda_1 \mathbb{I}_{\mathcal{X}} - \Psi_0^*\left(Z_0\right) & 0 \\ 0 & & 0 & \lambda_2 \mathbb{I}_{\mathcal{X}} - \Psi_1^*\left(Z_1\right) \end{pmatrix}.
\end{aligned}$$

Table 1: This table contains a standard form SDP for the maximum output fidelity. It can be shown to be equivalent to the above simpler form.

3.3.7 Quadratically constrained quadratic programming

In this subchapter we again restrict ourselves to the usual Euclidean space $\mathbb{C}^n$. According to S. Boyd and L. Vandenberghe [19] quadratically constrained quadratic program (QCQP) corresponds to the following optimization problem:

$$\begin{aligned} \text{minimize} \quad & \frac{1}{2}\langle x, P_0 x\rangle + \langle q_0, x\rangle + r_0, \\ \text{subject to} \quad & \frac{1}{2}\langle x, P_i x\rangle + \langle q_i, x\rangle + r_i \leq 0 \quad \text{for } i = 1, \ldots m, \\ & Ax = b. \end{aligned} \tag{55}$$

Here $P_i \in L(\mathbb{C}^n)$, $q_i, \in \mathbb{C}^n$, $r_i \in \mathbb{R}$ and $A:\ \mathbb{C}^n \to \mathbb{C}^m$ is an affine transformation. The vector $b \in \mathbb{C}^m$ resides in the output space of A which can be of arbitrary dimension $m \in \mathbb{N}$. In general, such a QCQP is NP-hard, because any $\{0,1\}$-integer problem can be brought into this form. Since problems of this kind are known to be NP-hard, the general QCQP-formulism has to be NP-hard as well.

If $P_0, \ldots, P_m \in \operatorname{Pos}(\mathbb{C}^n)$, then the corresponding QCQP is a convex optimization problem and can thus be solved efficiently. It corresponds to minimizing a convex objective function over an affine transformation of an intersection of ellipsoids, which is easily seen to be a convex set.

If a QCQP is non-convex, not all hope is lost. Convex relaxations of the problem allow for efficiently calculating bounds on the problem's optimal value. Here we present an SDP relaxation from [23]. For other relaxation methods we refer to [23, 24]. Our approach is based on the simple fact that for arbitrary $M \in L(\mathbb{C}^n)$, we can write $\langle x, Mx\rangle = \operatorname{tr}(XM)$ with $X = xx^*$. Therefore (55) can be rewritten in the following way:

$$\begin{aligned} \text{minimize} \quad & \frac{1}{2}\operatorname{tr}(XP_0) + \langle q_0, x\rangle + r_0, \\ \text{subject to} \quad & \frac{1}{2}\operatorname{tr}(XP_i) + \langle q_i, x\rangle + r_i \leq 0 \quad \text{for } i = 1, \ldots m, \\ & Ax = b, \\ & X = xx^*. \end{aligned}$$

This problem can directly be relaxed to a convex problem by replacing the nonconvex constraint $X = xx^*$ with the convex constraint $X \succeq xx^*$. By Schur's complement rule [19, 25], this generalized inequality constraint is equivalent to $\begin{pmatrix} X & x \\ x^* & 1 \end{pmatrix} \succeq 0$. Therefore, we obtain the following convex relaxation of (55):

$$\begin{aligned} \text{minimize} \quad & \frac{1}{2}\operatorname{tr}(XP_0) + \langle q_0, x\rangle + r_0, \\ \text{subject to} \quad & \frac{1}{2}\operatorname{tr}(XP_i) + \langle q_i, x\rangle + r_i \leq 0 \quad \text{for } i = 1, \ldots m, \\ & Ax = b, \\ & \begin{pmatrix} X & x \\ x^* & 1 \end{pmatrix} \succeq 0, \end{aligned}$$

which is an SDP. It can be brought into our standard primal SDP form (50) by multiplying the objective function with (-1) (i.e $P_0 \mapsto -P_0$, $q_0 \mapsto -q_0$ and $r_0 \mapsto -r_0$). The maximization of the new variables is then equivalent to minimizing the old ones. Finally we can turn the inequality constraints into equality constraints by introducing a slack variable[8] s_i for each $i = 1, \ldots, m$

$$\begin{array}{ll} \text{maximize} & \frac{1}{2}\mathrm{tr}\left(XP_0\right) + \langle q_0, x\rangle + r_0, \\ \text{subject to} & \frac{1}{2}\mathrm{tr}\left(XP_i\right) + \langle q_i, x\rangle - s_i + r_i = 0 \quad \text{for } i = 1, \ldots m, \\ & s_i \geq 0 \quad \text{for } i = 1, \ldots m, \\ & Ax = b, \\ & \begin{pmatrix} X & x \\ x^* & 1 \end{pmatrix} \succeq 0. \end{array}$$

Such an *SDP relaxation* yields a lower bound to the original NP-hard problem (55), which can be computed efficiently.

4 Our approach

4.1 POVM-norms

In this section, we introduce the main objective of our work – POVM norms. This norm concept was introduced by W. Matthews, S. Wehner and A. Winter in [4].

4.1.1 Identifying measurements with channels

As a starting point, we write an arbitrary informationally complete POVM measurement $\{M_k\}_{k=1}^n$ (see subsection 2.1.3 for the concrete definition) in the following way

$$\begin{array}{rcl} \widetilde{\mathcal{M}}: \ \mathrm{Herm}\left(\mathcal{X}\right) & \to & \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n \\ X & \mapsto & \sum_{k=1}^n |k\rangle \mathrm{tr}\left(M_k X\right). \end{array} \tag{56}$$

Here $\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ is the image of the mapping $\widetilde{\mathcal{M}}$. We can turn this mapping into a *measurement channel* by embedding the space of outcome vectors $\mathbb{R}^n$ diagonally in $\mathrm{Herm}\left(\mathcal{Y}\right)$ with $\mathcal{Y} \simeq \mathbb{C}^n$:

$$\begin{array}{rcl} \mathcal{M}: \ L\left(\mathcal{X}\right) & \to & \mathrm{Im}\left(\mathcal{M}\right) \subseteq \mathrm{Herm}\left(\mathcal{Y}\right) \\ X & \mapsto & \sum_{k=1}^n |k\rangle\langle k| \mathrm{tr}\left(M_k X\right). \end{array} \tag{57}$$

[8] The inequality $a \leq b$ is equivalent to demanding $a - s = b$ for some $s \geq 0$. Such a variable s is called slack variable.

This mapping is *completely positive*. The following short calculation shows that $\mathcal{M}$ also *preserves traces*. For any $X \in \mathrm{Herm}(\mathcal{X})$ we have

$$\begin{aligned} \mathrm{tr}\left(\mathcal{M}(X)\right) &= \mathrm{tr}\left(\sum_{k=1}^{n} |k\rangle\langle K| \mathrm{tr}\left(M_k X\right)\right) = \sum_{k=1}^{n} \mathrm{tr}\left(M_k X\right) \\ &= \mathrm{tr}\left(\left[\sum_{k=1}^{n} M_k\right] X\right) = \mathrm{tr}\left(\mathbb{I}_{\mathcal{X}} X\right) = \mathrm{tr}\left(X\right), \end{aligned}$$

where we have used the defining property (6) of a POVM. Therefore, the superoperator (57) is indeed a quantum channel. What is more, it is an *entanglement breaking channel.*

Due to the informational completeness of $\{M_k\}_{k=1}^{n}$ this channel is *injective* in the sense that $\mathcal{M}(X) \neq 0$ for any $X \neq 0$. Since $\mathcal{M}$ is also linear, it constitutes an *isomorphism* between $\mathrm{Herm}(\mathcal{X})$ and $\mathrm{Im}(\mathcal{M})$. It is clear that this isomorphic character holds for both measurement characterizations (56) and (57).

4.1.2 POVM norms

The channel $\mathcal{M}$ maps $\mathrm{Herm}(\mathcal{X})$ injectively onto a vector space $\mathrm{Herm}(\mathcal{Y})$ that is, in particular, endowed with the trace norm $\|.\|_1$. Hence, our measurement channel induces the following distance measure on the original space $\mathrm{Herm}(\mathcal{X})$:

$$\begin{aligned} \|X\|_{\mathcal{M}} &:= \|\mathcal{M}(X)\|_1 \quad \forall X \in \mathrm{Herm}(\mathcal{X}) \quad \text{or equivalently} && (58) \\ \|X\|_{\mathcal{M}} &:= \|\widetilde{\mathcal{M}}(X)\|_{l_1} \quad \forall X \in \mathrm{Herm}(\mathcal{X}). && (59) \end{aligned}$$

It is easy to see that both definitions are equivalent. We call $\|.\|_{\mathcal{M}}$ the *POVM norm* associated with the measurement $\{M_k\}_{k=1}^{n}$ that defines both $\mathcal{M}$ and $\widetilde{\mathcal{M}}$. The function $\|.\|_{\mathcal{M}} : \mathrm{Herm}(\mathcal{X}) \to \mathbb{R}$ really defines a norm. Indeed we have $\forall \alpha \in \mathbb{R}$ and $\forall X, Y \in \mathrm{Herm}(\mathcal{X})$

$$\begin{aligned} \|\alpha X\|_{\mathcal{M}} &= \|\mathcal{M}(\alpha X)\|_1 = \|\alpha \mathcal{M}(X)\|_1 = |\alpha| \|X\|_{\mathcal{M}} \quad \text{and} \\ \|X + Y\|_{\mathcal{M}} &= \|\mathcal{M}(X + Y)\|_1 = \|\mathcal{M}(X) + \mathcal{M}(Y)\|_1 \leq \|X\|_{\mathcal{M}} + \|Y\|_{\mathcal{M}}. \end{aligned}$$

Finally, non-degeneracy is assured via the informational completeness of the measurement $\mathcal{M}$ and non-degeneracy of the trace norm (for nonvanishing $X \in \mathrm{Herm}(\mathcal{X})$ we have $\mathcal{M}(X) \neq 0$ and consequently $\|\mathcal{M}(X)\|_1 \neq 0$).

Such POVM norms have operational significance in the field of state discrimination. Suppose that we have access to some measurement apparatus that is capable of scanning every state $\rho \in D(\mathcal{X})$ in an informationally complete way. This measurement apparatus shall correspond to a (necessarily informationally complete) single POVM $\{M_k\}_{k=1}^{n}$. We represent this measurement as a channel $\mathcal{M}$ via (57). We set ourselves the task of distinguishing a density operator $\rho \in D(\mathcal{X})$ from an alternative one $\sigma \in D(\mathcal{X})$. We have to take into account that the entire information accessible to us is given by the probability vectors $p = \mathcal{M}(\rho)$ and $q = \mathcal{M}(\sigma)$, respectively. It is easy to see that our optimal decision rule for this task is given by the maximum likelihood rule. Using idem rule, we get the following maximal probability of success:

$$P_{\text{success}} = \frac{1}{2} + \frac{1}{4}\sum_{k=1}^{n} |p_i - q_i| = \frac{1}{2} + \frac{1}{4}\|p - q\|_1 = \frac{1}{2} + \frac{1}{4}\|\mathcal{M}\left(\rho - \sigma\right)\|_1.$$

This almost looks like Helstrom's theorem [3] and gives an upper bound for the probability of correctly distinguishing the two systems. Hence, $\|.\|_{\mathcal{M}}$ is informationally significant. Rather than $\delta\left(\rho,\sigma\right) = \frac{1}{2}\|\rho - \sigma\|_1$ in Helstrom's original theorem, the bias is here given by $\frac{1}{2}\|\rho - \sigma\|_{\mathcal{M}}$. Both expressions are related via the obvious inequality

$$\frac{1}{2}\|\rho - \sigma\|_{\mathcal{M}} \leq \delta\left(\rho,\sigma\right) \quad \forall \rho,\sigma \in D\left(\mathcal{X}\right). \tag{60}$$

This inequality would surely turn into an equality if $\rho - \sigma \in \mathrm{Pos}\left(\mathcal{X}\right)$ (which requires either trivial $[\rho = \sigma]$ or unphysical $[\rho \notin D\left(\mathcal{X}\right)$ or $\sigma \notin D\left(\mathcal{X}\right)]$ quantum systems) and is usually strict otherwise. In all physical situations our bias is therefore usually smaller than the one given by Helstrom. This makes sense, because we only have access to a limited amount of measurements. In the theorem of Helstrom, on the other hand, all possible measurements are allowed.

4.1.3 POVM-norm constants

We can view inequality (60) as a manifestation of the non-optimality of our measurement $\mathcal{M}$. In this subsection we introduce a quantitative measure of this non-optimality in terms of norm constants. Such norm constants arise from the basic fact that in finite dimensional vector spaces all norms are equivalent. This implies that there exist constants $\tilde{\lambda}, \tilde{\mu} \in \mathbb{R}$ such that

$$\tilde{\lambda}\|X\|_1 \leq \|X\|_{\mathcal{M}} \leq \tilde{\mu}\|X\|_1 \quad \forall X \in L\left(\mathcal{X}\right). \tag{61}$$

This sandwich can be tightened by restricting it to traceless-operators $X \in \mathrm{L}_{\mathrm{tr}=0}\left(\mathcal{X}\right)$ which is the natural case in state discrimination. Since $\mathrm{L}_{\mathrm{tr}=0}\left(\mathcal{X}\right)$ is again a vector space, there exist $\mu, \lambda \in \mathbb{R}$ such that

$$\lambda\|X\|_1 \leq \|X\|_{\mathcal{M}} \leq \mu\|X\|_1 \quad \forall X \in \mathrm{L}_{\mathrm{tr}=0}\left(\mathcal{X}\right). \tag{62}$$

It is easy to see that $\lambda \geq \tilde{\lambda}$ and $\mu \leq \tilde{\mu}$ holds. Inequality (60), for instance, implies $\tilde{\mu} = 1$, whereas μ is usually smaller than 1. In [4] the authors could show the following relations

$$\frac{1}{2}\lambda \leq \tilde{\lambda} \leq \lambda, \tag{63}$$

$$\mu \leq \tilde{\mu} = 1. \tag{64}$$

Relation (64) is obvious and we present a novel proof of (63) in subsection 4.2.5. As already mentioned in the introduction, the norm constants λ and μ quantify the capabilities of our measurement POVM $\{M_k\}_{k=1}^{n}$.

- The constant λ can be seen as a *worst case promise* for arbitrary state discrimination: for distinguishing arbitrary states, the POVM measurement $\{M_k\}_{k=1}^n$ performs at least λ times as well as the corresponding optimal (Helstrom) measurement.
- Similarly μ corresponds to an *optimal case limitation*: The POVM measurement performs at most μ times as well as an optimal measurement for distinguishing arbitrary states.

It is clear that the constant λ is practically more relevant than μ. The remainder of this thesis is devoted to presenting 2 algorithms for bounding these constants. Our algorithms are computationally efficient and universally applicable. One approach readily yields the exact constants λ and $\tilde{\lambda}$ for certain families of POVM-measurements.

4.1.4 Inverse measurement mappings

Our algorithms rely on the highly artificial concept of *inverse measurement mappings.* As pointed out in subsection 4.1.1, any POVM measurement can be viewed as an isomorphic mapping (56)

$$\widetilde{\mathcal{M}}: \ \mathrm{Herm}(\mathcal{X}) \to \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n,$$

or an isomorphic channel

$$\mathcal{M}: \ \mathrm{Herm}\left(\mathcal{X}\right) \to \mathrm{Im}\left(\mathcal{M}\right) \subseteq \mathrm{Herm}\left(\mathcal{Y}\right).$$

Both maps are linear and bijective onto their image. Therefore they can be uniquely reversed by isomorphic inverse mappings:

$$\begin{aligned} \widetilde{\mathcal{M}}^{-1}: \ \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) &\to \mathrm{Herm}\left(\mathcal{X}\right) \quad \text{and} && (65)\\ \mathcal{M}^{-1}: \ \mathrm{Im}\left(\mathcal{M}\right) &\to \mathrm{Herm}\left(\mathcal{X}\right). && (66) \end{aligned}$$

that obey

$$\begin{aligned} \widetilde{\mathcal{M}}\left(\widetilde{\mathcal{M}}^{-1}\left(y\right)\right) &= y \quad \forall y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right), \quad \widetilde{\mathcal{M}}^{-1}\left(\widetilde{\mathcal{M}}\left(X\right)\right) = X \quad \forall X \in \mathrm{Herm}\left(\mathcal{X}\right),\\ \mathcal{M}\left(\mathcal{M}^{-1}\left(Y\right)\right) &= Y \quad \forall Y \in \mathrm{Im}\left(\mathcal{M}\right), \quad \mathcal{M}^{-1}\left(\mathcal{M}\left(X\right)\right) = X \quad \forall X \in \mathrm{Herm}\left(\mathcal{X}\right). \end{aligned}$$

This just means that each of the two mappings is both a left and a right inverse. The inverse superoperator $\mathcal{M}^{-1}$ preserves traces, since it is the inverse of a trace preserving map:

$$\mathrm{tr}\left(Y\right) = \mathrm{tr}\left(\mathcal{M}\left(\mathcal{M}^{-1}\left(Y\right)\right)\right) = \mathrm{tr}\left(\mathcal{M}^{-1}\left(Y\right)\right) \quad \forall Y \in \mathrm{Im}\left(\mathcal{M}\right).$$

It is easy to see, that the other inverse mapping $\widetilde{\mathcal{M}}$ has a similar property:

$$\langle 1, y\rangle = \mathrm{tr}\left(\widetilde{\mathcal{M}}^{-1}\left(y\right)\right), \tag{67}$$

where $1 = (1, \ldots, 1)^T \in \mathbb{R}^n$. However, unlike their reverse quantities which are completely positive, the inverse mappings even fail to be positive in general. The mapping $\mathcal{M}^{-1}$ therefore corresponds to a *Hermicity and trace preserving superoperator* in the general case. The mapping $\widetilde{\mathcal{M}}^{-1}$ has similar properties. We verify these properties at the end of the next subsection.

4.1.5 Explicit construction of $\widetilde{\mathcal{M}}^{-1}$

In this subsection we present an explicit construction of the mapping (65). We start by constructing an inverse channel $\widetilde{\mathcal{M}}^{-1}$ using the defining right inverse property $\widetilde{\mathcal{M}}\left(\widetilde{\mathcal{M}}_r^{-1}(y)\right) = y \ \forall y \in \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$ and an arbitrary basis $\{X_k\}_{k=1}^m$ of $\operatorname{Herm}(\mathcal{X})$. We then translate this mapping into a nice closed form.

We can characterize $\operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$ using $\{X_k\}_{k=1}^m$ in the following way:

$$\begin{aligned}\operatorname{Im}\left(\widetilde{\mathcal{M}}\right) &= \left\{\widetilde{\mathcal{M}}(X) : \ X \in \operatorname{Herm}(\mathcal{X})\right\} = \operatorname{span}\left\{\widetilde{\mathcal{M}}(X_1), \ldots, \widetilde{\mathcal{M}}(X_m)\right\} \\ &=: \operatorname{span}\{a_1, \ldots, a_m\} \subseteq \mathcal{Y}, \end{aligned} \tag{68}$$

where $a_i := \widetilde{\mathcal{M}}(X_i) \in \mathcal{Y}$ for $i = 1, \ldots, m$. Injectivity of $\widetilde{\mathcal{M}}$ implies that all vectors a_i are linearly independent and differ from zero. Hence they span $\operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$ and form a basis of this subspace. We now define the action of $\widetilde{\mathcal{M}}_r^{-1}$ on elements of $\operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$ via its action on the basis elements a_i:

$$\begin{aligned}\widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right] : \ \widetilde{\mathcal{A}} &\to \operatorname{Herm}(\mathcal{X}) \\ a_i &\mapsto X_i \quad \forall i = 1, \ldots, m. \end{aligned} \tag{69}$$

The argument $\left[\{X_i\}_i\right]$ makes the (seeming) dependence of our construction on the chosen basis explicit. Our inverse mapping therefore acts on a general element $y = \sum_{j=1}^m y_j a_j \in \widetilde{\mathcal{A}}$ in the following way:

$$\begin{aligned}\widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right](y) &= \widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right]\left(\sum_{j=1}^m y_j a_j\right) = \sum_{j=1}^m y_j \widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right](a_j) \\ &= \sum_{j=1}^m y_j X_j \in \operatorname{Herm}(\mathcal{X}).\end{aligned}$$

Note that this immediately implies:

$$\widetilde{\mathcal{M}}\left[\widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right](y)\right] = \widetilde{\mathcal{M}}\left(\sum_{j=1}^m y_j X_j\right) = \sum_{j=1}^m y_j \widetilde{\mathcal{M}}(X_j) = \sum_{j=1}^m y_j a_j = y.$$

Thus our construction (69) indeed fulfills the defining property of a right inverse mapping. However our construction appears to be basis dependent (which would indicate that it is not unique). This is actually not the case, as we now aim to show. In order to do so, let us pick a different basis $\{Z_i\}_{i=1}^m$ of $\mathrm{Herm}\left(\mathcal{X}\right)$. Following the same steps as before, this choice gives rise to a different basis $\{\tilde{a}_j\}_{j=1}^m$ of $\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$. This in turn results in an apparently different inverse mapping $\widetilde{\mathcal{M}}_r^{-1}\left[\{Z_i\}_i\right]$. We pick an arbitrary element $y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$and decompose it in two equivalent ways

$$y = \sum_{j=1}^m y_j a_j \quad \text{and} \quad y = \sum_{j=1}^m \tilde{y}_j \tilde{a}_j.$$

Consequently we have:

$$\widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right](y) = \sum_{j=1}^m y_j X_j \quad \text{and} \quad \widetilde{\mathcal{M}}_r^{-1}\left[\{Z_i\}_i\right] = \sum_{j=1}^m \tilde{y}_j Z_j.$$

Conversely we have by construction:

$$\begin{aligned} \widetilde{\mathcal{M}}\left(\sum_{j=1}^m y_j X_j\right) &= \widetilde{\mathcal{M}}\left[\widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right](y)\right] = y, \\ \widetilde{\mathcal{M}}\left(\sum_{j=1}^m \tilde{y}_j Z_j\right) &= \widetilde{\mathcal{M}}\left[\widetilde{\mathcal{M}}_r^{-1}\left[\{Z_i\}_i\right](y)\right] = y. \end{aligned}$$

Therefore $\widetilde{\mathcal{M}}\left(\sum_{j=1}^m y_j X_j\right) = \widetilde{\mathcal{M}}\left(\sum_{j=1}^m \tilde{y}_j Z_j\right)$ and injectivity of $\widetilde{\mathcal{M}}$ guarantees $\sum_{j=1}^m y_j X_j = \sum_{j=1}^m \tilde{y}_j Z_j := X$. Both mappings map any $y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ actually onto the same $X \in \mathrm{Herm}\left(\mathcal{X}\right)$. This allows us to identify both maps with each other:

$$\widetilde{\mathcal{M}}_r^{-1}\left[\{X_i\}_i\right] = \widetilde{\mathcal{M}}_r^{-1}\left[\{Z_i\}_i\right].$$

Since the bases $\{X_i\}_i$ and $\{Z_i\}_i$ could be chosen arbitrarily, this equivalence shows independence of the choice of basis used in (69). For this reason we omit the redundant argument $\left[\{X_i\}_i\right]$ from now on.

Our construction (69) already allows us to evaluate the action of $\widetilde{\mathcal{M}}_r^{-1}$ for any vector $y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ by following three steps:

1. Choose a basis $\{X_i\}_{i=1}^m$ of $\mathrm{Herm}\left(\mathcal{X}\right)$ and evaluate $a_i := \widetilde{M}\left(X_i\right)$.
2. Decompose y with respect to $\{a_j\}_{j=1}^m$: $y = \sum_{j=1}^m y_j a_j$.
3. $\widetilde{\mathcal{M}}_r^{-1}(y)$ is defined by its action onto the individual a_i's ($\widetilde{\mathcal{M}}_r^{-1}: a_i \mapsto X_i$):

$$\widetilde{\mathcal{M}}_r^{-1}(y) = \sum_{j=1}^m y_j \widetilde{\mathcal{M}}_r^{-1}\left(a_j\right) = \sum_{j=1}^m y_j X_j.$$

While this construction of $\widetilde{\mathcal{M}}_r^{-1}$ is essentially sufficient, it is difficult to bring the above procedure into a closed form. This inconvenience is due to the fact that the basis $\{a_j\}_{j=1}^m$ is in general not orthonormal. We can overcome this obstacle by orthonormalizing $\{a_j\}_{j=1}^m$ using the standard Gram-Schmidt procedure. This will result in an orthonormal basis $\{b_j\}_{j=1}^m$. However, since $\widetilde{\mathcal{M}}_r^{-1}$ has been defined with respect to the original basis $\{a_j\}_{j=1}^m$, we carefully have to keep track of all manipulations within the procedure. For this sake we introduce $m = \dim\left(\operatorname{Im}\left(\mathcal{M}\right)\right)$ linear maps

$$gs_i : \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \to \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \quad \text{for } i = 1, \ldots, m$$

that depend on i^2 scalar products $\langle a_k, a_l\rangle$ $k, l \leq i$ and i vectors $a_1, \ldots, a_i$. These functions are inductively defined as follows:

$$\begin{aligned}
gs_1 &= gs_1\left(\langle a_1, a_1\rangle; a_1\right) := \frac{a_1}{\|a_1\|_2}, \\
gs_2 &= gs_2\left(\langle a_k, a_l\rangle\ k, l \leq 2; a_1, a_2\right) := \frac{a_2 - \langle a_2, gs_1\rangle gs_1}{\|a_2 - \langle a_2, gs_1\rangle gs_1\|_2}, \\
&\vdots \\
gs_i &= gs_i\left(\langle a_k, a_l\rangle\ k, l \leq i;\ a_1, \ldots, a_i\right) := \frac{a_i - \sum_{j=1}^{i-1}\langle a_i, gs_j\rangle gs_j}{\|a_i - \sum_{j=1}^{i-1}\langle a_i, gs_j\rangle gs_j\|_2}, \\
&\vdots \\
gs_m &= gs_m\left(\langle a_k, a_l\rangle\ k, l \leq m;\ a_1, \ldots, a_m\right) := \frac{a_m - \sum_{j=1}^{m-1}\langle a_m, gs_j\rangle gs_j}{\|a_m - \sum_{j=1}^{m-1}\langle a_m, gs_j\rangle gs_j\|_2}.
\end{aligned}$$

Note that each such gs_i is linear in its vector arguments $a_1, \ldots, a_i$ which can be seen by inspection. The notation "gs" underlines the trivial connection between these maps and the Gram-Schmidt process. Setting

$$b_i := gs_i\left(\langle a_k, a_l\rangle\ k, l \leq i;\ a_1, \ldots, a_i\right) \tag{70}$$

yields an orthonormal basis $\{b_i\}_{i=1}^m$ of the linear subspace $\operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$. We stress out that each gs_i depends on numbers $\langle a_k, a_l\rangle$ and vectors a_k. The occuring numbers resemble scalar products of the form $\langle a_k, a_l\rangle$ and can be readily evaluated for any choice of POVM mapping $\widetilde{\mathcal{M}}$ and any basis $\{X_i\}_{i=1}^m$ of $\operatorname{Herm}\left(\mathcal{X}\right)$.

Our aim is now to use the ONB $\{b_i\}_{i=1}^m$ in order to write down $\widetilde{\mathcal{M}}_r^{-1}$ in a closed form. For this sake we note that our inverse channel acts on the first ONB-element b_1 in the following way:

$$\begin{aligned}
\widetilde{\mathcal{M}}_r^{-1}\left(b_1\right) &= \widetilde{\mathcal{M}}_r^{-1}\left(\frac{a_1}{\|a_1\|_2}\right) = \frac{\widetilde{\mathcal{M}}_r^{-1}\left(a_1\right)}{\|a_1\|_2} = \frac{X_1}{\|a_1\|_2} = gs_1\left(\langle a_1, a_1\rangle; X_1\right) \\
&:= Z_1\left(X_1\right) \in \operatorname{Herm}\left(\mathcal{X}\right).
\end{aligned}$$

And likewise for the second ONB-element we have:

$$\begin{aligned}
\widetilde{\mathcal{M}}_r^{-1}\left(b_2\right) &= \widetilde{\mathcal{M}}_r^{-1}\left(\frac{a_2-\langle a_2,gs_1\rangle gs_1}{\|a_2-\langle a_2,gs_1\rangle gs_1\|_2}\right)\\
&= \frac{\widetilde{\mathcal{M}}_r^{-1}\left(a_2\right)-\langle a_2,gs_1\rangle\widetilde{\mathcal{M}}_r^{-1}\left(gs_1\right)}{\|a_2-\langle a_2,gs_1\rangle gs_1\|_2}\\
&= \frac{X_2-\langle a_2,gs_1\rangle Z_1\left(X_1\right)}{\|a_2-\langle a_2,gs_1\rangle gs_1\|_2}\\
&= gs_2\left(\langle a_k,a_l\rangle\ k,l\leq 2;Z_1,X_2\right)\\
&=: Z_2\left(X_1,X_2\right)\in\mathrm{Herm}\left(\mathcal{X}\right),
\end{aligned}$$

because $\widetilde{\mathcal{M}}_r^{-1}\left(gs_1\right)=\widetilde{\mathcal{M}}_r^{-1}\left(b_1\right)=Z_1$. Inductively we can thus evaluate the action of $\widetilde{\mathcal{M}}_r^{-1}$ onto the i-th ONB-element:

$$\begin{aligned}
\widetilde{\mathcal{M}}_r^{-1}\left(b_i\right) &= \widetilde{\mathcal{M}}_r^{-1}\left(\frac{a_i-\sum_{j=1}^{i-1}\langle a_i,gs_j\rangle gs_j}{\|a_i-\sum_{j=1}^{i}\langle a_i,gs_j\rangle gs_j\|_2}\right)\\
&= \frac{\widetilde{\mathcal{M}}_r^{-1}\left(a_i\right)-\sum_{j=1}^{i-1}\langle a_i,gs_j\rangle\widetilde{\mathcal{M}}_r^{-1}\left(gs_j\right)}{\|a_i-\sum_{j=1}^{i-1}\langle a_i,gs_j\rangle gs_j\|_2}\\
&= \frac{X_i-\sum_{j=1}^{i-1}\langle a_i,gs_j\rangle Z_j\left(X_1,\ldots,X_j\right)}{\|a_i-\sum_{j=1}^{i}\langle a_i,gs_j\rangle gs_j\|_2}\\
&= gs_i\left(\langle a_k,a_l\rangle\ k,l\leq i;\ Z_1,\ldots Z_{i-1},X_i\right)\\
&=: Z_i\left(X_1,\ldots,X_i\right)\in\mathrm{Herm}\left(\mathcal{X}\right). \qquad (71)
\end{aligned}$$

For the sake of completeness we also present the image of the last element:

$$\begin{aligned}
\widetilde{\mathcal{M}}_r^{-1}\left(b_m\right) &= \widetilde{\mathcal{M}}_r^{-1}\left(\frac{a_i-\sum_{j=1}^{m-1}\langle a_i,gs_j\rangle gs_j}{\|a_i-\sum_{j=1}^{m-1}\langle a_i,gs_j\rangle gs_j\|_2}\right)\\
&= \frac{\widetilde{\mathcal{M}}_r^{-1}\left(a_i\right)-\sum_{j=1}^{m-1}\langle a_m,gs_j\rangle\widetilde{\mathcal{M}}_r^{-1}\left(gs_j\right)}{\|a_i-\sum_{j=1}^{m-1}\langle a_m,gs_j\rangle gs_j\|_2}\\
&= \frac{X_m-\sum_{j=1}^{m-1}\langle a_m,gs_j\rangle Z_m}{\|a_i-\sum_{j=1}^{m-1}\langle a_m,gs_j\rangle gs_j\|_2}\\
&= gs_m\left(\langle a_k,a_l\rangle\ k,l\leq m;\ Z_1,\ldots,Z_{m-1},X_m\right)\\
&=: Z_m\left(X_1,\ldots,X_m\right)\in\mathrm{Herm}\left(\mathcal{X}\right).
\end{aligned}$$

In our definition of the Z_i's – the images of the individual b_i's under $\widetilde{\mathcal{M}}_r^{-1}$ – we have replaced the vectorial arguments $a_i\in\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ in each gs_i by Hermitian matrix arguments $X_i\in\mathrm{Herm}\left(\mathcal{X}\right)$. This replacement turns our original endomorphism $gs_i:\ \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)\rightarrow\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ into a different one:

$$gs_i\left(\langle a_k,a_l\rangle\ k,l\leq i;\ X_1,\ldots,X_i\right):\ \mathrm{Herm}\left(\mathcal{X}\right)\quad\rightarrow\quad\mathrm{Herm}\left(\mathcal{X}\right).$$

By a slight abuse of notation we use the same name for this mapping. We furthermore stress out that the Z_i's are in general not positive semidefinite, which is obvious given their construction. This manifests the non-positive character of $\widetilde{\mathcal{M}}_r^{-1}$.

The ONB elements b_i with $i = 1, \ldots, m$ of $\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ and their images $Z_i = \widetilde{\mathcal{M}}_r^{-1}(b_i) \in L(\mathcal{X})$ now finally allow us to write down the desired mapping in a neat closed form:

$$\begin{aligned} \widetilde{\mathcal{M}}_r^{-1} : \widetilde{\mathcal{A}} &\rightarrow L(\mathcal{X}), \\ y &\mapsto \sum_{j=1}^{m} Z_j \langle b_j, y \rangle. \end{aligned} \tag{72}$$

Note that this assertion indeed guarantees the defining property of a right inverse mapping for each $y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$. In order to see this, let us focus on an arbitrary ONB element b_i with $i = 1, \ldots, m$:

$$\begin{aligned} \widetilde{\mathcal{M}}\left[\widetilde{\mathcal{M}}_r^{-1}(b_i)\right] &= \widetilde{\mathcal{M}}\left(\sum_{j=1}^{m} Z_j \langle b_j, b_i \rangle\right) = \widetilde{\mathcal{M}}(Z_i) \\ &= \widetilde{\mathcal{M}}\left(gs_i\left(\langle a_k, a_l \rangle\ k,l \leq i;\ X_1, \ldots, X_i\right)\right) \\ &= gs_i\left(\langle a_k, a_l \rangle\ k,l \leq i;\ \widetilde{\mathcal{M}}(X_1), \ldots, \widetilde{\mathcal{M}}(X_i)\right) \\ &= gs_i\left(\langle a_k, a_l \rangle\ k,l \leq i;\ a_1, \ldots, a_m\right) \\ &= b_i, \end{aligned}$$

where we have used the fact that gs_i is linear in the second line and the definitions of a_k and b_i. Since (72) is by construction a right inverse for each such ONB-element b_i , linearity implies that it does so for arbitrary $y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$.

4.1.6 Explicit construction of $\mathcal{M}^{-1}$

In the previous subsection we derived the closed form expression (72) for $\widetilde{\mathcal{M}}^{-1}$. We can translate this into an explicit expression for $\mathcal{M}^{-1}$ (see formula (66)) by embedding the diagonal subspace of $\mathrm{Herm}(\mathcal{Y})$ in $\mathbb{R}^n$

$$\begin{aligned} E : \mathrm{Herm}(\mathcal{Y}) &\rightarrow \mathbb{R}^n, \\ Y &\mapsto \sum_{l=1}^{n} \mathrm{tr}\left(|e_l\rangle\langle e_l| Y\right) |e_l\rangle. \end{aligned} \tag{73}$$

Combining (72) with (73) indeed yields the desired mapping, because E maps $\mathrm{Im}\left(\mathcal{M}^{-1}\right) \subseteq \mathrm{Herm}(\mathcal{Y})$ isomorphically onto $\mathrm{Im}\left(\widetilde{\mathcal{M}}^{-1}\right) \subseteq \mathbb{R}^n$. This indeed implies

$$\mathcal{M}^{-1} := \widetilde{\mathcal{M}}^{-1} \circ E : \qquad \mathrm{Im}\left(\mathcal{M}^{-1}\right) \overset{E}{\rightarrow} \mathrm{Im}\left(\widetilde{\mathcal{M}}^{-1}\right) \overset{\widetilde{\mathcal{M}}^{-1}}{\rightarrow} \mathrm{Herm}(\mathcal{X}).$$

Our desired inverse superoperator has the following closed form for any $Y \in \operatorname{Herm}(\mathcal{Y})$

$$\begin{aligned}\mathcal{M}^{-1}: \quad & \operatorname{Im}\left(\mathcal{M}^{-1}\right) \to \operatorname{Herm}(\mathcal{X}), \\ \mathcal{M}^{-1}(Y) \quad &= \sum_{j=1}^{m} Z_j \langle b_j, \sum_{l=1}^{n} \langle e_l, Y e_l \rangle | e_l \rangle \\ &= \sum_{j=1}^{m} \sum_{l=1}^{n} Z_j \langle b_j, e_l \rangle \operatorname{tr}\left(|e_l\rangle\langle e_l| Y\right). \end{aligned} \tag{74}$$

Note that this superoperator is bijective between $\operatorname{Im}(\mathcal{M}) \subseteq \operatorname{Herm}(\mathcal{Y})$ and $\operatorname{Herm}(\mathcal{X})$. However, expression (74) is actually defined on the entire space $\operatorname{Herm}(\mathcal{Y})$, where it acts trivially on elements that lie in the orthogonal complement of $\operatorname{Im}(\mathcal{M})$, (i.e. $\mathcal{M}^{-1}(Y) = 0 \ \forall Y \in \operatorname{Im}(\mathcal{M})^{\perp}$). Therefore it makes sense to consider the following continuation of $\mathcal{M}^{-1}$

$$\mathcal{M}^{-1}_{\text{continuation}} := \mathcal{M}^{-1} \circ \mathcal{P}_{\operatorname{Im}(\mathcal{M})} : \ \operatorname{Herm}(\mathcal{Y}) \to \operatorname{Herm}(\mathcal{X}),$$

where $\mathcal{P}_{\operatorname{Im}(\mathcal{M})}$ denotes the orthogonal projector onto $\operatorname{Im}(\mathcal{M})$. By a slight abuse of notation, we will denote this continuation simply $\mathcal{M}^{-1}$. The closed expression (74) already corresponds to this continuation.

4.2 The polytope approach

In this section we present approaches for calculating or at least bounding the norm constants $\tilde{\lambda}$ in (61) and λ in (62). In order to do so, we first present a formula for obtaining $\tilde{\lambda}$ which corresponds to maximizing a convex function over a convex polytope – hence the name “polytope approach”. The main idea behind this approach is to use the theorem from section 2.2 in order to access this convex polytope optimization. All this is done in subsection 4.2.1. A slight modification of our formula allows for calculating the refined constant λ instead of $\tilde{\lambda}$. This modification is the scope of subsection 4.2.2. The computational complexity of both algorithms is then analyzed in 4.2.3. We furthermore relax the optimization and obtain computationally cheap upper and lower bounds for the desired norm constants in 4.2.4. Finally, we apply our formalism to SIC-POVM measurements. This allows us to analytically obtain the exact corresponding constants λ and $\tilde{\lambda}$. This calculation is original and refines the bounds from [4].

4.2.1 The exact algorithm for $\tilde{\lambda}$

We can rewrite the lower inequality in chain (2) in the following way:

$$\|X\|_1 \leq \frac{1}{\tilde{\lambda}} \|X\|_{\widetilde{\mathcal{M}}} \quad \forall X \in \operatorname{Herm}(\mathcal{X}).$$

From this we infer that $\frac{1}{\tilde{\lambda}}$ is the solution of an optimization problem

$$\begin{aligned} \frac{1}{\tilde{\lambda}} &= \sup\left\{\|X\|_1 :\ \|X\|_{\mathcal{M}} = 1,\ X \in \mathrm{Herm}\left(\mathcal{X}\right)\right\} \\ &= \max\left\{\|X\|_1 :\ \|X\|_{\mathcal{M}} \leq 1,\ X \in \mathrm{Herm}\left(\mathcal{X}\right)\right\}. \end{aligned} \tag{75}$$

This expression corresponds to maximizing a convex function ($X \mapsto \|X\|_1$) over a convex set (the norm ball $B\left(\|.\|_{\mathcal{M}}\right)$). Therefore sup = max and the maximum is acquired on the boundary of the convex set. However this boundary is just characterized by $\|X\|_{\mathcal{M}} = 1$, which is why the second equality sign in (75) holds. We point out that, due to the definition of $\|.\|_{\mathcal{M}}$, this actually means

$$\frac{1}{\tilde{\lambda}} = \max\left\{\|X\|_1 :\ \|\widetilde{\mathcal{M}}\left(X\right)\|_1 \leq 1,\ X \in \mathrm{Herm}\left(\mathcal{X}\right)\right\}.$$

We now use the surjectivity of the inverse mapping $\widetilde{\mathcal{M}}^{-1} :\ \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \to \mathrm{Herm}\left(\mathcal{X}\right)$ (65) (which satisfies $\widetilde{\mathcal{M}}\left(\widetilde{\mathcal{M}}^{-1}\left(y\right)\right) = y\ \forall y \in \mathbb{R}^n$) in order to alter our maximization problem to

$$\begin{aligned} \frac{1}{\tilde{\lambda}} &= \max\left\{\|X\|_1 :\ \|\widetilde{\mathcal{M}}\left(X\right)\|_1 \leq 1,\ X \in \mathrm{Herm}\left(\mathcal{X}\right)\right\} \\ &= \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ \|\widetilde{\mathcal{M}}\left(\widetilde{\mathcal{M}}^{-1}\left(y\right)\right)\|_1 \leq 1,\ y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n\right\} \\ &= \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ \|y\|_1 \leq 1,\ y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n\right\} \\ &= \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ y \in B\left(\|.\|_1\right) \cap \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n\right\}. \end{aligned} \tag{76}$$

Recall that $\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ is a linear subspace of $\mathbb{R}^n$ and thus an unbounded convex polyhedron. Therefore its intersection with the bounded polyhedron $B\left(\|.\|_1\right)$ is again a convex polyhedron. We denote the resulting object $B\left(\|.\|_1\right) \cap \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$. Due to the Weyl-Minkowski theorem (see subsection 3.1.6), our set of interest $\mathcal{B}$ is also a convex polytope. This is characterized by l vertices $v_1, \ldots, v_l$:

$$B\left(\|.\|_1\right) \cap \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) = \mathrm{conv}\left(v_1, \ldots, v_l\right). \tag{77}$$

We will discuss the computational complexity of this polyhedron-polytope characterization in the next but one subsection. Here we only mention that the overall number of vertices l naturally depends the measurement $\{M_k\}_{k=1}^n$, so indeed $l = l\left(\{M_k\}_{k=1}^n\right)$. This allows us to rewrite the above characterization of $\frac{1}{\tilde{\lambda}}$ in the following way:

$$\frac{1}{\tilde{\lambda}} = \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ y \in \mathrm{conv}\left(v_1, \ldots, v_l\right)\right\}.$$

This expression still corresponds to maximizing a convex function over a convex set which is in general NP hard. However, due to the polytopic description of our feasible set, the theorem of section 2.2 is applicable and tells us that we in fact have

$$\frac{1}{\tilde{\lambda}} = \max_{i=1,\ldots,l} \|\widetilde{\mathcal{M}}^{-1}(v_i)\|_1. \tag{78}$$

Note that the function $y \mapsto \|\widetilde{\mathcal{M}}^{-1}(y)\|_1$ can be evaluated efficiently for any $y \in \mathbb{R}^n$. Therefore, calculating $\tilde{\lambda}$ via (78) is feasible, provided that the number of vertices l does not explode and the vertices $v_1, \ldots, v_l$ themselves can be obtained efficiently.

4.2.2 The exact algorithm for λ

The measurement mapping $\widetilde{\mathcal{M}}$ is the commutative version of an entanglement breaking channel $\mathcal{M}$. In particular, such a channel preserves traces. We already showed in (67) that the commutative mapping $\widetilde{\mathcal{M}}$ obeys the corresponding property

$$\langle 1, \widetilde{\mathcal{M}}(X) \rangle = \operatorname{tr}(X) \quad \forall X \in \operatorname{Herm}(\mathcal{X}),$$

where $1 = (1, \ldots, 1)^T \in \mathbb{R}^n$. Hence, $\widetilde{\mathcal{M}}$ maps traceless operators $X \in L_{\operatorname{tr}=0}(\mathcal{X})$ onto vectors $y \in \mathbb{R}^n$ that obey $\langle 1, y \rangle = 0$. We denote this space

$$L_{\langle 1,.\rangle=0} \quad = \quad \{y \in \mathbb{R}^n : \langle 1, y \rangle = 0\} \subseteq \mathbb{R}^n.$$

Adding the condition $y \in L_{\langle .,1\rangle=0}$ to (76) is equivalent to demanding traceless operators in the original maximization. This yields a formula for the refined norm constant λ, namely

$$\frac{1}{\lambda} = \max\left\{ \|\widetilde{\mathcal{M}}^{-1}(y)\|_1 : \ y \in B(\|.\|_1) \cap L_{\langle .,1\rangle=0} \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n \right\}. \tag{79}$$

The intersection $B(\|.\|_1) \cap L_{\langle .,1\rangle=0}$ is a polytope whose vertex representation can be obtained analytically. In order to do so, we will use our insights from subsection 3.1.6 about the vertices and edges of the cross polytope. A (minimal) half space representation of the intersection polytope is given by

$$B(\|.\|_1) \cap L_{\langle .,1\rangle=0} = \{x \in \mathbb{R}^n : \ \langle 1, x \rangle = 0, \ \langle c, x \rangle \leq 1, \ c = (\pm 1, \ldots, \pm 1)\} \tag{80}$$

and contains $2^n + 2$ linear inequalities[9]. Note that not a single vertex e_i of the original cross polytope lies in this intersection. This allows us to discard them in this discussion. However, any point $x \in B(\|.\|_1) \cap L_{\langle .,1\rangle=0}$ exactly satisfies the inequality $\langle 1, x \rangle \geq 0$ (or equivalently $\langle 1, x \rangle \leq 0$). From this we can conclude that any vertex of the intersection has to lie on an edge of the cross polytope. This is because any vertex has to exactly satisfy n linear independent inequalities from the polytope's half space characterization (see subsection 3.1.6 and [18], Chapter III, Theorem 4.2). A point in the intersection can only achieve this if it exactly satisfies at least $(n-1)$ linearly independent inequalities of the original cross polytope characterization. Since vertices do not count, this is only possible for points lying on some edge[10] of $B(\|.\|_1)$. We have shown in equation (37)

[9] This is because the equality $\langle 1, x \rangle = 0$ is equivalent to the two linearly dependent inequalities $\langle 1, x \rangle \leq 0$ and $\langle 1, x \rangle \geq 0$.

[10] Recall that we have defined an edge to be a set that exactly satisfies $(n-1)$ linearly independent defining inequalities of the polytope.

(subsection 3.1.6) that all edges of the cross polytope are of the form

$$l(\tau) = \tau(\pm e_i) + (1-\tau)(\pm e_j) \quad \text{for } i \neq j,\ \tau \in [0,1].$$

The intersections of these lines with the subspace $L_{\langle .,1\rangle=0}$ are easily seen to establish the following set

$$\left\{ \pm \frac{1}{2}(e_i - e_j) \right\}_{i \neq j}$$

that contains $2n(n-1)$ vectors. Each of them is obviously a vertex of $B(\|.\|_1) \cap L_{\langle 1,.\rangle=0}$. Our discussion above furthermore assures that this set of vertices is indeed complete. Hence, we can characterize our polytope of interest using the vertex representation:

$$B(\|.\|_1) \cap L_{\langle 1,.\rangle=0} = \operatorname{conv}\left(\left\{ \pm \frac{1}{2}(e_i - e_j) \right\}_{i \neq j} \right).$$

This vertex characterization allows us to immediately obtain an exact formula for λ:

$$\frac{1}{\lambda} = \max \left\{ \|\widetilde{\mathcal{M}}^{-1}(y)\|_1 : \quad y \in \operatorname{conv}\left(\left\{ \pm \frac{1}{2}(e_i - e_j) \right\}_{i \neq j} \right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n \right\}.$$

This formula again depends crucially on the intersection of a polytope ($\operatorname{conv}\left(\left\{ \pm \frac{1}{2}(e_i - e_j) \right\}_{i \neq j} \right)$) with a subspace ($\operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$). Such an intersection is again a polytope and can be characterized by l' vertices

$$\operatorname{conv}\left(\left\{ \pm \frac{1}{2}(e_i - e_j) \right\}_{i \neq j} \right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) = \operatorname{conv}\left(v_1', \ldots, v_l'\right). \tag{81}$$

Using the theorem from subsection 2.2 once more results in

$$\frac{1}{\lambda} = \max_{i=1,\ldots,l'} \|\widetilde{\mathcal{M}}^{-1}\left(v_i'\right)\|_1, \tag{82}$$

which is the traceless equivalent of (78).

4.2.3 Computational complexity

The sole computationally critical step in the above algorithms is obtaining the convex polytope description (77) of $B(\|.\|_1) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$, or the description (81) of $B(\|.\|_1) \cap L_{\langle .,1\rangle=0} \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$, respectively. This task corresponds to efficiently computing the intersection of two polytopes. It is a special case of the famous "vertex enumeration problem" [26]. K. Fukuda discusses this special case in [27].

He points out that calculating intersections can be done efficiently, provided that both polytopes are given in halfspace representation. In this case one can simply take the union of both defining inequality sets and do redundancy removal.

If one polytope (or both) is (are) given in vertex representation, the situation is much more challenging. A polynomial algorithm is known for a special case of polytope intersections [28]. In order to be efficient, this algorithm requires that the polytopes are in "general position". However, it can also be applied to general polytopes. We refer to [28] for a proper definition of the general position property. H. Raj Tiwary could show in [29] that the general intersection problem is NP-hard if at least one polytope is given in vertex representation.

Unfortunately, our problem exactly corresponds to this case, because the 1-norm ball $B\left(\|.\|_1\right)$ can only be efficiently represented in vertex representation. Furthermore our setting does not admit the general position property. The critical step of obtaining the vertex representations of our intersections is thus hard for general subspaces.

4.2.4 Cheap upper and lower bounds for $\tilde{\lambda}$ and λ

In this subsection we present a way of bounding the constants $\tilde{\lambda}$ and λ. The bounds presented are computationally cheap in the sense that they can be efficiently computed. Let us start with bounding the constant $\tilde{\lambda}$. In the preceding subsection we pointed out that classifying the intersection polytope $B\left(\|.\|_1\right) \cap \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ is the only hard step in our approach. This (possibly) tedious evaluation can be omitted, if we consider simple convex sub- and supersets of $B\left(\|.\|_1\right) \cap \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ instead of evaluating the set itself. In order to obtain such sets, we introduce the orthogonal projector $\mathcal{P} := \mathcal{P}_{\mathcal{Y}}^{\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)} \,:\, L\left(\mathcal{Y}\right) \to \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$ that projects onto the subspace $\mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$. We point out that the following inclusion series holds:

$$\mathrm{conv}\left(\pm\frac{\mathcal{P}e_1}{\left\|\mathcal{P}e_1\right\|_1}, \ldots, \pm\frac{\mathcal{P}e_n}{\left\|\mathcal{P}e_n\right\|}\right) \subseteq B\left(\|.\|_1\right) \cap \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathrm{conv}\left(\pm\mathcal{P}e_1, \ldots, \pm\mathcal{P}e_n\right), \tag{83}$$

which is easy to see. Let us start with showing the first inclusion by considering an arbitrary convex combination $y = \sum_{i=1}^n \sum_{\pm} \alpha_i^{\pm} \frac{\pm\mathcal{P}e_i}{\left\|\mathcal{P}e_i\right\|_1}$, where $\sum_{i=1}^n \sum_{\pm} \alpha_i^{\pm} = 1$ and $a_i^+, a_i^- \geq 0$ for each $i = 1, \ldots n$. Obviously $y = \mathcal{P} \sum_{i=1}^n \sum_{\pm} \alpha_i^{\pm} \frac{\pm e_i}{\left\|\mathcal{P}e_1\right\|_i}$ which immediately implies $y \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$. Furthermore note that

$$\|y\|_1 = \left\| \sum_{i=1}^n \sum_{\pm} \alpha_i^{\pm} \frac{\pm\mathcal{P}e_i}{\left\|\mathcal{P}e_i\right\|_1} \right\|_1 \leq \sum_{i=1}^n \sum_{\pm} \alpha_i^{\pm} \frac{\left\|\pm\mathcal{P}e_i\right\|}{\left\|\mathcal{P}e_i\right\|_1} = \sum_{i=1}^n \sum_{\pm} \alpha_i^{\pm} = 1.$$

This implies $y \in B\left(\|.\|_1\right)$ as well and we have shown the first inclusion. For the second inclusion, we simply note that we have $z = \mathcal{P}z$ for each $z \in \mathrm{Im}\left(\widetilde{\mathcal{M}}\right)$.

Combining this with $B\left(\|.\|_1\right) = \operatorname{conv}\left\{\pm e_1, \ldots, \pm e_n\right\}$ immediately implies that for each $z \in B\left(\|.\|_1\right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$, we have

$$z \in \mathcal{P}\operatorname{conv}\left(\pm e_1, \ldots, \pm e_n\right) = \operatorname{conv}\left(\pm \mathcal{P}e_1, \ldots, \pm \mathcal{P}e_n\right).$$

This proves the second inclusion.

Note that the above set inclusions are usually strict. This follows from the fact that orthogonal projectors in general do not contract the l_1-norm[11].

The first inclusion in (83) allows us to relax our exact maximization formula (76):

$$\begin{aligned}
\frac{1}{\tilde{\lambda}} &= \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 : \ y \in B\left(\|.\|_1\right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n\right\} \\
&\geq \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 : \ y \in \operatorname{conv}\left(\pm\frac{\mathcal{P}e_1}{\|\mathcal{P}e_1\|_1}, \ldots, \pm\frac{\mathcal{P}e_n}{\|\mathcal{P}e_n\|}\right) \subseteq \mathbb{R}^n\right\} \\
&= \max_{1 \leq i \leq n}\left\|\widetilde{\mathcal{M}}^{-1}\left(\frac{\mathcal{P}e_i}{\|\mathcal{P}e_i\|_1}\right)\right\|_1 = \max_{1 \leq i \leq n}\frac{\left\|\widetilde{\mathcal{M}}^{-1}\left(\mathcal{P}e_i\right)\right\|_1}{\|\mathcal{P}e_i\|_1},
\end{aligned}$$

where we have once more used our theorem from section 2.2. Similarly, we can use the second inclusion in (83) to obtain a converse bound:

$$\begin{aligned}
\frac{1}{\tilde{\lambda}} &= \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 : \ y \in B\left(\|.\|_1\right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n\right\} \\
&\leq \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 : \ y \in \operatorname{conv}\left(\pm\mathcal{P}e_1, \ldots, \pm\mathcal{P}e_n\right) \subseteq \mathbb{R}^n\right\} \\
&= \max_{1 \leq i \leq n}\|\widetilde{\mathcal{M}}^{-1}\left(\mathcal{P}e_i\right)\|_1.
\end{aligned}$$

These two estimates allow us to bound the inverse of the sought for constant $\tilde{\lambda}$:

$$\max_{1 \leq i \leq n}\frac{\left\|\widetilde{\mathcal{M}}^{-1}\left(\mathcal{P}e_i\right)\right\|_1}{\|\mathcal{P}e_i\|_1} \leq \frac{1}{\tilde{\lambda}} \leq \max_{1 \leq i \leq n}\left\|\widetilde{\mathcal{M}}^{-1}\left(\mathcal{P}e_i\right)\right\|_1. \tag{84}$$

We can obtain a similar cheap sandwich for the restricted norm constant λ by following a completely analogue procedure:

$$\max_{i \neq j}\frac{\left\|\widetilde{\mathcal{M}}^{-1}\left(\mathcal{P}e_i - \mathcal{P}e_j\right)\right\|_1}{\|\mathcal{P}e_i - \mathcal{P}e_j\|_1} \leq \frac{1}{\lambda} \leq \max_{i \neq j}\frac{1}{2}\left\|\widetilde{\mathcal{M}}^{-1}\left(\mathcal{P}e_i - \mathcal{P}e_j\right)\right\|_1. \tag{85}$$

It is obvious that the bounds in these two sandwich inequalities are computationally cheap to obtain. However, (84) and (85) are in general not likely to be

[11] Take $e_1 \in \mathbb{R}^2$ and $\mathcal{P} = |v\rangle\langle v|$ with $v = \frac{1}{\sqrt{1+\epsilon^2}}\left(1, \epsilon\right)$ and $\epsilon > 0$ as an example. In this case we have $\|\mathcal{P}e_1\|_1 = \|\langle v, e_1\rangle v\|_1 = \|v\|_1 = \frac{1+\epsilon}{\sqrt{1+\epsilon^2}}$. This expression is greater than 1, provided that ϵ is sufficiently small.

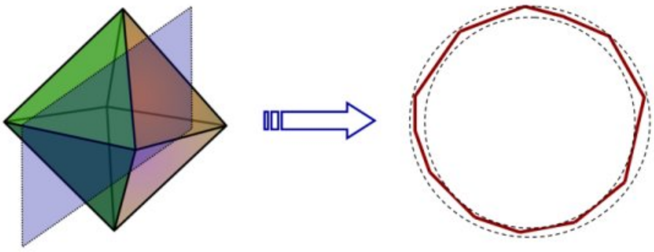


Figure 3: Pictorial illustration of Dvoretzky's theorem. It indicates that the intersections of the cross polytope and a subspace of certain size almost resemble an ellipsoid (circle) in sufficiently large dimensions. The graphic is taken from a blog entry [31] by J. Lee in tcs math.

very tight. We illustrate this for (84) by considering Dvoretzky's theorem. To be more precise, we use the setting that V. Milman used to prove idem theorem in [30]: If $B \subseteq \mathbb{R}^n$ is an arbitrary convex body and H is a random $c(\epsilon)\log n$-dimensional hyperplane through the origin, then with high probability, $B \cap H$ ϵ-close to an ellipsoid. This astonishing fact is illustrated in figure 3. Applied to our situation, this theorem implies that our set of interest $B(\|.\|_1) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$ is very likely to be almost an ellipsoid, provided that our measurement POVM $\{M_k\}_{k=1}^n$ is sufficiently redundant (in the sense that $\dim \operatorname{Herm}(\mathcal{X}) \approx \log(n)$). In our inclusion (83), we then aim to approximate this almost ellipsoidal object by "honest" polytopes (that only possess up to n vertices). It is obvious that such an approximation cannot be very accurate. Naturally, this inaccuracy propagates into (84). Basically the same argument also holds for (85).

Note that our Dvoretzky-argument also underlines the (general) computational hardness of calculating the vertices of $B(\|.\|_1) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$. Indeed if the polytope $B(\|.\|_1) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$ almost looks like an ellipsoid, it has to have many vertices. Calculating these objects is thus likely to be hard, simply because so many of them need to be computed.

We conclude this subsection by giving a worst case promise for the upper bounds in (84) and (85). It is based on the simple observation that any orthogonal projector $\mathcal{P}$ obeys

$$\|\mathcal{P}v\|_1 \leq \sqrt{n}\|\mathcal{P}v\|_2 \leq \sqrt{n}\|v\|_2 \quad \forall v \in \mathbb{R}^n.$$

Hence, we conclude $\mathcal{P}e_i \in \sqrt{n}B\left(\|.\|_1\right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$ and consequently

$$\begin{aligned}
\max_{1\leq i\leq n}\left\|\widetilde{\mathcal{M}}^{-1}\left(\mathcal{P}e_i\right)\right\|_1 &= \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ y\in \operatorname{conv}\left(\pm\mathcal{P}e_1,\ldots,\pm\mathcal{P}e_n\right)\right\} \\
&\leq \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ y\in \sqrt{n}B\left(\|.\|_1\right)\cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\right\} \\
&= \sqrt{n}\max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ y\in B\left(\|.\|_1\right)\cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\right\} \\
&= \sqrt{n}\frac{1}{\tilde{\lambda}}.
\end{aligned}$$

An analogous reasoning can also be applied to (85). We conclude that the above sandwich inequalities yield lower bounds on λ and $\tilde{\lambda}$ that have a worst case accuracy of $\frac{1}{\sqrt{n}}$.

4.2.5 The relation between λ and $\tilde{\lambda}$

In this section we derive relation (3) which shows that the constants λ and $\tilde{\lambda}$ are equivalent up to a factor of 2:

$$\frac{1}{2}\tilde{\lambda} \leq \lambda \leq \tilde{\lambda}.$$

The second inequality follows directly from comparing the corresponding maximization procedures (76) and (79):

$$\begin{aligned}
\frac{1}{\lambda} &= \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ y\in B\left(\|.\|_1\right)\cap L_{\langle .,1\rangle=0}\cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\subseteq\mathbb{R}^n\right\} \\
&\leq \max\left\{\|\widetilde{\mathcal{M}}^{-1}\left(y\right)\|_1 :\ y\in B\left(\|.\|_1\right)\cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\subseteq\mathbb{R}^n\right\} \\
&= \frac{1}{\tilde{\lambda}}.
\end{aligned}$$

In order to show the lower bound, we introduce the projector $\mathcal{P}_{\langle .,1\rangle=0} : \mathbb{R}^n \to L_{\langle .,1\rangle=0}$. This operator is explicitly given by

$$\mathcal{P}_{\langle .,1\rangle=0} = \mathbb{I}_{\mathbb{R}^n} - \frac{1}{n}|1\rangle\langle 1|,$$

where again $1 = (1,\ldots,1)^T$. Using this expression, we can readily evaluate the projector's influence onto the l_1-norm of a given vector. It suffices to consider its action on the standard basis vectors

$$\begin{aligned}
\left\|\mathcal{P}_{\langle .,1\rangle=0}|e_i\rangle\right\|_{l_1} &= \left\||e_i\rangle - \frac{1}{n}\langle 1,e_i\rangle|1\rangle\right\|_{l_1} = \left\||e_i\rangle - \frac{1}{n}|1\rangle\right\|_{l_1} \\
&= \left\|-\frac{1}{n}\left(1,\ldots,1,1-n,1,\ldots,1\right)^T\right\|_{l_1} \\
&= 2\frac{n-1}{n} \leq 2 \quad \forall i=1,\ldots n.
\end{aligned}$$

We know from subsection 4.2.4 (inclusion relation 83) that we can find an upper bound for λ by approximating $B\left(\|.\|_1\right) \cap L_{\langle .,1\rangle=0}$ via its superset $\operatorname{conv}\left(\pm\mathcal{P}_{\langle .,1\rangle=0}e_1,\ldots,\pm\mathcal{P}_{\langle .,1\rangle=0}e_n\right)$. However, together with our previous calculation, this yields the following simple superset:

$$B\left(\|.\|_1\right) \cap L_{\langle .,1\rangle=0} \subseteq \operatorname{conv}\left(\pm\mathcal{P}_{\langle .,1\rangle=0}e_1,\ldots,\pm\mathcal{P}_{\langle .,1\rangle=0}e_n\right) \subseteq 2B\left(\|.\|_1\right).$$

We can use this inclusion to obtain

$$\begin{aligned}
\frac{1}{\lambda} &= \max\left\{\left\|\widetilde{\mathcal{M}}^{-1}(y)\right\| :\ y \in \left(B\left(\|.\|_1\right) \cap L_{\langle .,1\rangle=0}\right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\right\} \\
&\leq \max\left\{\left\|\widetilde{\mathcal{M}}^{-1}(y)\right\| :\ y \in 2B\left(\|.\|_1\right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\right\} \\
&= 2\max\left\{\left\|\widetilde{\mathcal{M}}^{-1}(y)\right\| :\ y \in B\left(\|.\|_1\right) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\right\} \\
&= 2\frac{1}{\tilde{\lambda}}.
\end{aligned}$$

This is just our desired formula (3). W. Matthews and his collaborators already derived this relation in [4] via a direct estimation. Their calculation relies on a clever, but not very intuitive, rewriting of the considered state. Our proof follows a simple geometric procedure and is therefore more intuitive than the original one.

4.2.6 Exact constants $\tilde{\lambda}$ and λ for SIC-POVMs

In this subsection we analytically calculate $\tilde{\lambda}$ and λ for a special family of POVM's, namely SIC-POVMs [32]. We obtain explicit expressions for the norm constants by using formulas (78) and (82) .

A SIC-POVM is an informationally complete POVM that is endowed with a special symmetry property. Furthermore such a POVM is exactly informationally complete in the sense that it consists of exactly d^2 different elements. Throughout this subsection we consider a Hilbert space $\mathbb{C}^d$. This implies that the state space $\operatorname{Herm}\left(\mathbb{C}^d\right)$ has real dimension d^2. The elements $\{F_i\}_{i=1}^{d^2}$ of a SIC POVM correspond to subnormalized projectors $F_i = \frac{1}{d}|\psi_i\rangle\langle\psi_i|$ (where $\langle\psi_i,\psi_i\rangle = 1\ \forall i = 1,\ldots,d^2$). The symmetry property corresponds to demanding a constant equal inner product between the elements:

$$\operatorname{tr}\left(F_iF_j\right) = \frac{c^2}{d^2} \quad i \neq j.$$

Here $c^2 \in \mathbb{R}_+$ denotes the required constant overlap. The constant c^2 is uniquely defined by another defining property ($\sum_{i=1}^{d^2} F_i = \mathbb{I}_{\mathbb{C}^d}$) of the SIC-POVM. It can be easily shown that $c^2 = \frac{1}{d+1}$ must hold. Hence we get the formulas

$$\begin{aligned} \operatorname{tr}(F_i F_j) &= \frac{1}{d^2(d+1)} \quad i \neq j, \\ \operatorname{tr}(F_i F_i) &= \frac{1}{d^2}, \\ \sum_{i=1}^{d^2} F_i &= \mathbb{I}_{\mathbb{C}^d}, \\ F_i &\geq 0. \end{aligned}$$

Note that the exact informational completeness implies that our measurement mapping

$$\begin{aligned} \widetilde{\mathcal{M}} : \operatorname{Herm}\left(\mathbb{C}^d\right) &\to \mathbb{R}^{d^2}, \\ X &\mapsto \sum_{k=1}^{d^2} |k\rangle \operatorname{tr}(F_k X) \end{aligned}$$

is already surjective ($\operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \simeq \mathcal{X}$). This in turn implies $B_1(\|.\|_1) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right) = B_1(\|.\|_1)$ and we can avoid the computationally hard step of calculating the intersection. Consequently we get

$$\begin{aligned} \frac{1}{\bar{\lambda}} &= \max\left\{ \|\widetilde{\mathcal{M}}^{-1}(y)\|_1 : \ y \in B(\|.\|_1) \subseteq \mathbb{R}^{d^2} \right\} \\ &= \max_{i=1,\dots d^2} \|\widetilde{\mathcal{M}}^{-1}(e_i)\|_1 \end{aligned}$$

which can be evaluated analytically. We do this by picking the SIC POVM $\{F_1, \dots, F_{d^2}\}$ itself as a basis of $\operatorname{Herm}(\mathcal{X})$. We can calculate the image $\widetilde{\mathcal{M}}(F_i)$ of each basis element F_i:

$$\begin{aligned} \alpha_i &:= \widetilde{\mathcal{M}}(F_i) = \sum_{k=1}^{d^2} |k\rangle \operatorname{tr}(F_k F_i) = |i\rangle \operatorname{tr}(F_i F_i) + \sum_{k \neq i} |k\rangle \operatorname{tr}(F_k F_i) \\ &= \frac{1}{d^2}|i\rangle + \sum_{k \neq i} \frac{1}{d^2(d+1)}|k\rangle = \frac{1}{d^2(d+1)} \left((d+1)\,|i\rangle + \sum_{k \neq i} |k\rangle \right) \\ &= \frac{1}{d^2(d+1)} \left(d|i\rangle + \sum_{k=1}^{d^2} |k\rangle \right) \quad \forall i = 1 \dots, d^2. \end{aligned}$$

It is easy to see that the vectors $\alpha_1, \dots, \alpha_{d^2}$ form a basis of $\mathbb{R}^{d^2}$ and the action of the inverse mapping $\widetilde{\mathcal{M}}^{-1}$ corresponds to

$$\begin{aligned} \widetilde{\mathcal{M}}^{-1} : \mathbb{R}^{d^2} &\to \operatorname{Herm}\left(\mathbb{C}^d\right), \\ \alpha_i &\mapsto F_i \quad \forall i = 1, \dots, d^2. \end{aligned}$$

In order to obtain $\tilde{\lambda}$, we have to check the value of $\widetilde{\mathcal{M}}$ at each vertex point $\pm e_i$ with $i = 1 \ldots, d^2$. Observing

$$\begin{aligned}\sum_{j=1}^{d^2} \alpha_j &= \sum_{j=1}^{d^2} \frac{1}{d^2 (d+1)} \left(d|j\rangle + \sum_{k=1}^{d^2} |k\rangle \right) = \frac{1}{d^2 (d+1)} \left(d \sum_{j=1}^{d^2} |j\rangle + \sum_{k=1}^{d^2} |k\rangle \sum_{j=1}^{d^2} 1 \right) \\ &= \frac{1}{d^2 (d+1)} \left(d + d^2 \right) \sum_{j=1}^{d^2} |j\rangle = \frac{1}{d} \sum_{j=1}^{d^2} |j\rangle\end{aligned}$$

allows us to find the representation of each standard basis vector in the basis $(\alpha_1, \ldots, \alpha_{d^2})$:

$$e_i = d (d+1) \alpha_i - \sum_{j=1}^{d^2} \alpha_j. \tag{86}$$

From this we can immediately infer that

$$\widetilde{\mathcal{M}}^{-1} (e_i) = d (d+1) F_i - \sum_{j=1}^{d^2} F_j = (d+1) |\psi_i\rangle\langle\psi_i| - \mathbb{I}_{\mathbb{C}^d} \quad \forall i = 1, \ldots, d^2.$$

Since this matrix is already diagonal, we can use the pinching inequality to obtain its trace norm:

$$\begin{aligned}\left\| \widetilde{\mathcal{M}}^{-1} (e_i) \right\|_1 &= \|(d+1) |\psi_i\rangle\langle\psi_i| - \mathbb{I}_{\mathbb{C}^d}\|_1 \\ &= d \left\| |\psi_i\rangle\langle\psi_i| \right\|_1 + \left\| \mathbb{I}_{\mathbb{C}^d} - |\psi_i\rangle\langle\psi_i| \right\|_1 \\ &= d + (d-1) = 2d - 1.\end{aligned}$$

This expression is equal for all standard basis vectors and thus also corresponds to the maximum. Hence, we can infer that

$$\tilde{\lambda} = \frac{1}{2d-1}. \tag{87}$$

For obtaining the refined constant λ, we have to check the vertices $\pm\frac{1}{2}(e_i - e_j)$ with $i \neq j$, $i, j = 1, \ldots, d^2$ of the polytope $B(\|.\|_1) \cap L_{\langle .,1\rangle = 0}$, instead of checking the vertices $\pm e_i$ of $B(\|.\|_1)$. From (86) we can directly infer

$$\frac{1}{2}(e_i - e_j) = \frac{1}{2} d (d+1) (\alpha_i - \alpha_j) \quad \forall i, j = 1, \ldots, d^2.$$

Similar to above, we conclude

$$\begin{aligned}\left\| \widetilde{\mathcal{M}}^{-1} \left(\pm\frac{1}{2} (e_i - e_j) \right) \right\|_1 &= \frac{1}{2} d (d+1) \|F_i - F_j\|_1 \\ &= \frac{1}{2} (d+1) \left\| |\psi_i\rangle\langle\psi_i| - |\psi_j\rangle\langle\psi_j| \right\|_1 \\ &= \frac{1}{2} (d+1) \frac{2d}{d+1} = d.\end{aligned}$$

This value is again a constant that does not depend on i, j. Therefore the maximization is once more trivial and we obtain

$$\lambda = \frac{1}{d}. \tag{88}$$

In [4], the authors also consider SIC POVM's as a special case of 2-designs. Their bound amounts to

$$\frac{1}{2\,(d+1)} \leq \lambda \leq \frac{1}{d}.$$

Our result for $\tilde{\lambda}$ yields the weaker lower bound $\frac{1}{4d-2}$ for this sandwich via the basic relation $\frac{1}{2}\tilde{\lambda} \leq \lambda$. However, formula (88) is much stronger. It states that the upper bound $\frac{1}{d}$ is actually always acquired which makes the whole inequality redundant. W. Matthews and his collaborators considered the specific state difference $\rho - \sigma = |\psi_1\rangle\langle\psi_i| - |\psi_2\rangle\langle\psi_2|$. For this special case they could show $\|\mathcal{M}\,(\rho - \sigma)\,\|_1 = \frac{1}{d}\|\rho - \sigma\|_1$, which implies $\lambda \leq \frac{1}{d}$. Such a bare case study can however only yield a bound on the desired constant λ. Our formalism gives additional structure to their choice of state. It implies that the $\rho - \sigma$ above is indeed extremal (a worst case scenario), because it is the image of the vertex $\frac{1}{2}\,(e_1 - e_2)$ under $\widetilde{\mathcal{M}}^{-1}$. This insight allows us to render the inequality $\lambda \leq \frac{1}{d}$ into an equality $\lambda = \frac{1}{d}$.

Finally, we point out the obvious fact that our results are compatible in the sense that they fulfill $\tilde{\lambda} \leq \lambda$ and $\frac{1}{2}\lambda \leq \tilde{\lambda}$.

4.2.7 Discussion

Our polytope algorithm for obtaining $\tilde{\lambda}$ (see subsection 4.2.1) crucially depends on the geometric structure of $B\,(\|.\|_1) \cap \operatorname{Im}\left(\widetilde{\mathcal{M}}\right)$. Its computational complexity scales with the number of vertices l of the intersection polytope[12]. This is because algorithms for obtaining these vertices [26, 28] have polynomial output sensitivity. Furthermore our maximization procedure requires checking a function's value at each vertex.

The worst case scaling of l with respect to the dimensions n and m is not yet fully understood. Dvoretzky's theorem (see subsection 4.2.4) indicates that the number l is very likely to be huge if $n \gg m$. This, as well as certain case studies, suggest a scaling which is exponentially dominated by the codimension $(n-m)$ of the subspace $\operatorname{Im}\left(\widetilde{\mathcal{M}}\right) \subseteq \mathbb{R}^n$. To rigorously prove this conjecture for general subspaces, however, seems to be difficult. One strategy is to find an explicit worst case m-dimensional subspace for each $1 \leq m \leq n$. Characterizing the corresponding intersection polytope would then yield a tight upper bound onto the scaling of l. Such worst case realizations are interesting on their own and finding them would constitute an interesting follow up task.

[12] Recall that $n = \dim\left(B\,(\|.\|_1)\right)$ denotes the number of POVM measurements, whereas $m = \dim\left(\operatorname{Im}\left(\widetilde{\mathcal{M}}\right)\right) = \dim L\,(\mathcal{X})$ denotes the dimension of the operator space considered.

The difficulty of characterizing intersection polytopes vanishes in the special case of exactly informationally complete POVMS. Such measurements obey $n = m$ and we have $\mathrm{Im}\left(\widetilde{\mathcal{M}}\right) \simeq \mathbb{R}^n$ which consequently implies $B\left(\|.\|_1\right) \cap \mathrm{Im}\left(\widetilde{\mathcal{M}}\right) = B\left(\|.\|_1\right)$. Hence, we can completely avoid the (potentially tedious) step of calculating intersection vertices and directly maximize our objective function over all cross polytope vertices $\pm e_1, \ldots, \pm e_n$. Naturally, this can be readily done. One important special case of such exactly informationally complete measurements are SIC POVMs. Due to their additional symmetry we could analytically calculate $\lambda = \frac{1}{d}$ and $\tilde{\lambda} = \frac{1}{2d-1}$, where d is the dimension of the underlying Hilbert space. This original result tightens the previously known bound $\frac{1}{2}\frac{1}{d+1} \leq \lambda \leq \frac{1}{d}$ from [4] and adds deeper understanding to their reasoning (see subsection 4.2.6).

The other side of the coin is of course, that the polytope approach is likely to perform bad, if $n \gg m$. This is the case, if the measurement POVM is characterized by a lot of redundancy. However, in this situation not all hope is lost yet. If the POVM has high degree of symmetry, the intersection polytope is likely to be much simpler than our worst case discussion from above suggests. Preprocessing in the form of a clever redundancy removal could make obtaining reasonable bounds on λ and $\tilde{\lambda}$ feasible. Exploiting these ideas would constitute an interesting follow-up project.

4.3 The diamond approach

This approach uses the channel description $\mathcal{M}: \mathrm{Herm}\left(\mathcal{X}\right) \to \mathrm{Herm}\left(\mathcal{Y}\right)$ of our measurement. We show in subsection 4.3.1 that the refined norm constants μ and λ are in one-to-one correspondence with induced 1-norms of artificial superoperators solely depending on $\{M_k\}_{k=1}^n$. In subsection 4.3.2 we show that the induced 1-norm can be written as a (non-convex) QCQP. We apply an SDP relaxation to this program in subsection 4.3.3 in order to obtain bounds on λ and μ which can be efficiently calculated. Converse bounds can be found on a fidelity based level by applying the Fuchs-van de Graaf inequalities. This is shown in subsection 4.3.4. Finally, we give some comments about the tightness of our estimates in a discussion that concludes this section.

4.3.1 The exact algorithm

On the contrary to the previous approach, we focus here on the channel description of our measurement POVM $\{M_k\}_{k=1}^n$

$$\begin{aligned} \mathcal{M}: \mathrm{Herm}\left(\mathcal{X}\right) &\to \mathrm{Herm}\left(\mathcal{Y}\right) \\ X &\mapsto \sum_{k=1}^n |k\rangle\langle k| \mathrm{tr}\left(M_k X\right) \end{aligned}$$

and its inverse counterpart

$$\mathcal{M}^{-1}: \mathrm{Herm}\left(\mathcal{Y}\right) \to \mathrm{Herm}\left(\mathcal{X}\right)$$

whose explicit description is given by (74). Our aim is to get a formula for the norm constants in (62)

$$\lambda \|X\|_1 \leq \|X\|_{\mathcal{M}} \leq \mu \|X\|_1.$$

In order to do so, we write

$$\begin{aligned} \mu &= \sup \left\{ \|X\|_{\mathcal{M}} : \ \|X\|_1 = 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \\ &= \max \left\{ \|X\|_{\mathcal{M}} : \ \|X\|_1 \leq 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \\ &= \max \left\{ \|\mathcal{M}\,(X)\,\|_1 : \ \|X\|_1 \leq 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \end{aligned}$$

and similarly

$$\begin{aligned} \frac{1}{\lambda} &= \sup \left\{ \|X\|_1 : \ \|X\|_{\mathcal{M}} = 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \\ &= \max \left\{ \|X\|_1 : \ \|X\|_{\mathcal{M}} \leq 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \\ &= \max \left\{ \|X\|_1 : \ \|\mathcal{M}\,(X)\,\|_1 \leq 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\}. \end{aligned}$$

The second equalities in both expressions hold because each case corresponds to maximizing a convex function over a convex set. In each equality chain the third equality follows from definition (58) ($\|X\|_{\mathcal{M}} = \|\mathcal{M}\,(X)\,\|_1 \ \forall X \in \mathrm{Herm}\,(\mathcal{X})$). Now recall that $\mathcal{M}^{-1} : \ \mathrm{Im}\,(\mathcal{M}) \to \mathrm{Herm}\,(\mathcal{X})$ is surjective and trace preserving. Therefore we can write

$$\begin{aligned} \frac{1}{\lambda} &= \max \left\{ \|X\|_1 : \ \|\mathcal{M}\,(X)\,\|_1 \leq 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \\ &= \max \left\{ \|\mathcal{M}^{-1}\,(Y)\,\|_1 : \ \|\mathcal{M}\left(\mathcal{M}^{-1}\,(Y)\right)\|_1 \leq 1, \ \mathrm{tr}\left(\mathcal{M}^{-1}\,(Y)\right) = 0, \ Y \in \mathrm{Im}\,(\mathcal{M}) \right\} \\ &= \max \left\{ \|\mathcal{M}^{-1}\,(Y)\,\|_1 : \ \|Y\|_1 \leq 1, \ \mathrm{tr}\,(Y) = 0, \ Y \in \mathrm{Im}\,(\mathcal{M}) \right\}. \end{aligned}$$

This already looks very similar to the μ-formula. Now we introduce orthogonal projectors

$$\begin{aligned} \mathcal{P}_{\mathcal{X}}^{\mathrm{tr}=0} : \ \mathrm{Herm}\,(\mathcal{X}) &\to L_{\mathrm{tr}=0}\,(\mathcal{X}) \subseteq \mathrm{Herm}\,(\mathcal{Y})\,, \\ \mathcal{P}_{\mathcal{Y}}^{\mathrm{tr}=0} : \ \mathrm{Herm}\,(\mathcal{Y}) &\to L_{\mathrm{tr}=0}\,(\mathcal{Y}) \subseteq \mathrm{Herm}\,(\mathcal{Y}) \quad \text{as well as} \\ \mathcal{P}_{\mathcal{Y}}^{\mathrm{Im}(\mathcal{M})} : \ \mathrm{Herm}\,(\mathcal{Y}) &\to \mathrm{Im}\,(\mathcal{M}) \subseteq \mathrm{Herm}\,(\mathcal{Y})\,. \end{aligned}$$

The first two operators resemble projectors onto the tracefree subspaces of $\mathcal{X}$ and $\mathcal{Y}$, respectively (i.e. $\mathrm{tr}\left(\mathcal{P}_{\mathcal{X}}^{\mathrm{tr}=0}\,(X)\right) = 0 \ \forall X \in \mathrm{Herm}\,(\mathcal{X})$ and $\mathrm{tr}\left(\mathcal{P}_{\mathcal{X}}^{\mathrm{tr}=0}\,(Y)\right) = 0$ $\forall Y \in \mathrm{Herm}\,(\mathcal{Y})$), whereas the last one corresponds to the orthogonal projector onto the image of $\mathcal{M}$ which is a linear subspace of $\mathrm{Herm}\,(\mathcal{Y})$. Using them we can write

$$\begin{aligned} \mu &= \max \left\{ \|\mathcal{M}\,(X)\,\|_1 : \ \|X\|_1 \leq 1, \ \mathrm{tr}\,(X) = 0, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \\ &= \max \left\{ \left\|\mathcal{M}\left(\mathcal{P}_{\mathcal{X}}^{\mathrm{tr}=0}\,(X)\right)\right\|_1 : \ \|X\|_1 \leq 1, \ X \in \mathrm{Herm}\,(\mathcal{X}) \right\} \end{aligned}$$

and likewise

$$\begin{aligned} \frac{1}{\lambda} &= \max \left\{ \|\mathcal{M}^{-1}\,(Y)\,\|_1 : \ \|Y\|_1 \leq 1, \ \mathrm{tr}\,(Y) = 0, \ Y \in \mathrm{Im}\,(\mathcal{M}) \right\} \\ &= \max \left\{ \left\|\mathcal{M}^{-1}\left(\mathcal{P}_{\mathcal{Y}}^{\mathrm{tr}=0}\,(Y)\right)\right\|_1 : \ \|Y\|_1 \leq 1, \ Y \in \mathrm{Im}\,(\mathcal{M}) \right\} \\ &= \max \left\{ \left\|\mathcal{M}^{-1}\left(\mathcal{P}_{\mathcal{Y}}^{\mathrm{tr}=0}\left(\mathcal{P}_{\mathcal{Y}}^{\mathrm{Im}(\mathcal{M})}\,(Y)\right)\right)\right\|_1 : \ \|Y\|_1 \leq 1, \ Y \in \mathrm{Herm}\,(\mathcal{Y}) \right\} \end{aligned}$$

We simplify these results by defining the following *hermicity preserving, trace annihilating* superoperators:

$$\begin{aligned} \Phi_\mu &:= \mathcal{M} \circ \mathcal{P}_{\mathcal{X}}^{\mathrm{tr}=0} : \quad \mathrm{Herm}(\mathcal{X}) \to \mathrm{Herm}(\mathcal{Y}) && (89) \\ \Phi_\lambda &:= \mathcal{M}^{-1} \circ \mathcal{P}_{\mathcal{Y}}^{\mathrm{tr}=0} \circ \mathcal{P}_{\mathcal{Y}}^{\mathrm{Im}(\mathcal{M})} : \quad \mathrm{Herm}(\mathcal{Y}) \to \mathrm{Herm}(\mathcal{X}). && (90) \end{aligned}$$

Note that Φ_μ and Φ_λ solely depend on the underlying POVM $\{M_k\}_{k=1}^n$ and can be explicitly constructed (see subsection 4.1.6). With this notation we indeed get

$$\begin{aligned} \mu &= \max\{\|\Phi_\mu(X)\|_1 : \|X\|_1 \leq 1, \ X \in \mathrm{Herm}(\mathcal{X})\} = \|\Phi_\mu\|_1, \\ \frac{1}{\lambda} &= \max\{\|\Phi_\lambda(Y)\|_1 : \|Y\|_1 \leq 1, \ Y \in \mathrm{Herm}(\mathcal{Y})\} = \|\Phi_\lambda\|_1. \end{aligned}$$

Therefore the sought for quantities really correspond to induced 1-norms of the superoperators Φ_μ and Φ_λ.

4.3.2 A QCQP for calculating the induced 1 norm

In this subsection we present a QCQP for calculating the induced 1-norm of an arbitrary superoperator $\Phi \in T(\mathcal{X}, \mathcal{Y})$. Our quadratic program is inspired by J. Watrous' SDP for the diamond norm [10, 11]. We assume that this superoperator is given by a Stinespring pair $A_0, A_1 \in L(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ such that

$$\Phi(X) = \mathrm{tr}_{\mathcal{Z}}(A_0 X A_1^*). \tag{91}$$

Recall that, due to convexity, we can write the induced 1-norm as

$$\|\Phi\|_1 = \max\{\|\Phi(|x\rangle\langle y|)\|_1 : \ x, y \in S(\mathcal{X})\}$$

(see subsection 2.1.7 , formula (13)). The following algorithm yields the negative square $\left(-\|\Phi\|_1^2\right)$ of the sought for induced 1-norm:

$$\begin{aligned} \text{minimize:} \quad & \langle x, -A_1 A_1^* x\rangle && (92) \\ \text{subject to:} \quad & \mathrm{tr}_{\mathcal{Y}}(|x\rangle\langle x|) = \mathrm{tr}_{\mathcal{Y}}(A_0 |u\rangle\langle u| A_0^*), \\ & u \in S(\mathcal{X}), \\ & x \in \mathcal{Y} \otimes \mathcal{Z}. \end{aligned}$$

The objective function is indeed a quadratic function in x. However it is manifestly non-convex, because $(-A_1 A_1^*)$ is negative semidefinite. This is the reason why this program cannot be implemented efficiently. We propose a convex relaxation of this problem in the next subsection. The constraints are quadratic equalities, which can be turned into the canonical form of a QCQP.

We now prove that this algorithm indeed yields $\left(-\|\Phi\|_1^2\right)$ for any superoperator Φ given by (91). Let us define our set of interest in the following way:

$$\mathcal{A} := \{|x\rangle\langle x| : \ x \in \mathcal{Y} \otimes \mathcal{Z}, \ \mathrm{tr}_{\mathcal{Y}}(|x\rangle\langle x|) = \mathrm{tr}_{\mathcal{Y}}(A_0|u\rangle\langle u|A_0^*) \text{ for some } u \in S(\mathcal{X})\}. \tag{93}$$

The optimization result $(-\alpha) := \min_{x\in\mathcal{A}}\langle A_1A_1^*, |x\rangle\langle x|\rangle$ of the above optimization is equivalent to the following expression:

$$\alpha = \max_{x\in\mathcal{A}}\langle A_1A_1^*, |x\rangle\langle x|\rangle.$$

Note that by definition we have

$$\begin{aligned}
\|\Phi\|_1^2 &= \max_{u,v\in S(\mathcal{X})} \|\Phi\left(\|u\rangle\langle v|\right)\|_1^2 = \max_{u,v\in S(\mathcal{X})} \|\mathrm{tr}_{\mathcal{Z}}\left(A_0|u\rangle\langle v|A_1^*\right)\|_1^2 \\
&= \max_{\substack{u,v\in S(\mathcal{X})\\ U\in U(\mathcal{Y})}} \left|\mathrm{tr}\left(U\mathrm{tr}_{\mathcal{Z}}\left[A_0|u\rangle\langle v|A_1^*\right]\right)\right|^2 \\
&= \max_{\substack{u,v\in S(\mathcal{X})\\ U\in U(\mathcal{Y})}} \left|\mathrm{tr}\left(\left[U\otimes\mathbb{I}_{\mathcal{Z}}\right]A_0|u\rangle\langle v|A_1^*\right)\right|^2 \\
&= \max_{\substack{u,v\in S(\mathcal{X})\\ U\in U(\mathcal{Y})}} \left|\langle v|A_1^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0|u\rangle\right|^2 \\
&= \max_{\substack{u\in S(\mathcal{X})\\ U\in U(\mathcal{Y})}} \|A_1^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0u\|_2^2 \\
&= \max_{\substack{u\in S(\mathcal{X})\\ U\in U(\mathcal{Y})}} \mathrm{tr}\left[A_1^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0|u\rangle\langle u|A_0^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)^*A_1\right] \\
&= \max_{\substack{u\in S(\mathcal{X})\\ U\in U(\mathcal{Y})}} \mathrm{tr}\left[A_1A_1^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0|u\rangle\langle u|A_0^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)^*\right] \\
&= \max_{\substack{u\in S(\mathcal{X})\\ U\in U(\mathcal{Y})}} \langle A_1A_1^*, \left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0|u\rangle\langle u|A_0^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)^*\rangle.
\end{aligned}$$

Apart from standard tricks, we here have used formula (5) ($\|X\|_1 = \max_{U\in U(\mathcal{X})}|\langle U, X\rangle|$) for the trace distance, the self polarity (24) of the 2-norm ($\|x\|_2 = \max_{\|y\|_2\leq 1}\langle x, y\rangle$) and the basic fact that $\|Sx\|_2^2 = \mathrm{tr}\left(S|x\rangle\langle x|S^*\right) = \mathrm{tr}\left(S^*S|x\rangle\langle x|\right)$ holds.

It therefore makes sense to define the set

$$\mathcal{B} := \left\{\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0|u\rangle\langle u|A_0^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)^* :\ u\in S(\mathcal{X}),\ U\in U(\mathcal{Y})\right\}.$$

We now have to show that $\mathcal{A} = \mathcal{B}$. This can be done by showing two converse inclusions.

1. $\mathcal{B}\subseteq\mathcal{A}$: Let us pick $u\in S(\mathcal{X})$ and $U\in U(\mathcal{Y})$ arbitrarily and set:

   $$x = \left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0u.$$

   Then xx^* is pure by construction and we furthermore have

   $$\mathrm{tr}_{\mathcal{Y}}\left(|x\rangle\langle x|\right) = \mathrm{tr}_{\mathcal{Y}}\left[\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)A_0|u\rangle\langle u|A_0^*\left(U\otimes\mathbb{I}_{\mathcal{Z}}\right)^*\right] = \mathrm{tr}_{\mathcal{Y}}\left(A_0|u\rangle\langle u|A_0^*\right),$$

which according to (93) implies $X \in \mathcal{A}$.

2. $\mathcal{A} \subseteq \mathcal{B}$: Conversely, let us consider an arbitrary element $x \in \mathcal{A}$ and a corresponding $u \in S(\mathcal{X})$ such that

$$\operatorname{tr}_{\mathcal{Y}}(|x\rangle\langle x|) = \operatorname{tr}_{\mathcal{Y}}(A_0|u\rangle\langle u|A_0^*).$$

Now both x and $A_0 u$ are purifications of the same state $(\operatorname{tr}_{\mathcal{Y}}(|x\rangle\langle x|))$. Hence they are unitarily equivalent in the sense that there exists a $U \in U(\mathcal{Y})$ such that:

$$x = (U \otimes \mathbb{I}_{\mathcal{Z}}) A_0 u.$$

But this just means that:

$$|x\rangle\langle x| = (U \otimes \mathbb{I}_{\mathcal{Z}}) A_0|u\rangle\langle u|A_0^* (U \otimes \mathbb{I}_{\mathcal{Z}})^*$$

and therefore $x \in \mathcal{B}$.

This finishes the proof of the validity of our QCQP (92). □

4.3.3 The diamond norm as proxy for our induced 1-norm QCQP

Note that our QCQP (92) does not change if we replace the demand $u \in S(\mathcal{X})$ by the equivalent conditions $\operatorname{tr}(|u\rangle\langle u|) = 1$ and $u \in \mathcal{X}$. Therefore the problem is equivalent (modulo flipping a sign) to

$$\begin{aligned} \text{maximize:} \quad & \langle x, A_1 A_1^* x\rangle \\ \text{subject to:} \quad & \operatorname{tr}_{\mathcal{Y}}(|x\rangle\langle x|) = \operatorname{tr}_{\mathcal{Y}}(A_0|u\rangle\langle u|A_0^*), \\ & \operatorname{tr}(|u\rangle\langle u|) = 1, \\ & u \in \mathcal{X}, \\ & x \in \mathcal{Y} \otimes \mathcal{Z}. \end{aligned}$$

In subsection 3.3.7 we have shown how such a QCQP can be relaxed to an SDP. This is done by replacing $|x\rangle\langle x|$ and$|u\rangle\langle u|$ by X and ρ, as well as imposing the SDP constraint $X \succeq |x\rangle\langle x|$, $(\rho \succeq |u\rangle\langle u|)$. This leads to the following relaxation

$$\begin{aligned} \text{maximize} \quad & \langle A_1 A_1^*, X\rangle \\ \text{subject to} \quad & \operatorname{tr}_{\mathcal{Y}}(X) = \operatorname{tr}_{\mathcal{Y}}(A_0 \rho A_0^*), \\ & \operatorname{tr}(\rho) = 1 \\ & X \succeq |x\rangle\langle x|, \\ & \rho \succeq |u\rangle\langle u|, \\ & u \in \mathcal{X}, \\ & x \in \mathcal{Y} \otimes \mathcal{Z}. \end{aligned}$$

Note that the original variables x and u do not appear in the actual process. The boundary condition $X \succeq |x\rangle\langle x|$ for at least one $x \in \mathcal{Y} \otimes \mathcal{Z}$ can therefore safely be replaced by the condition $X \succeq 0$. Similarly, we can simply write $\rho \succeq 0$

and drop u. However, positive semidefiniteness of ρ together with the condition $\operatorname{tr}(\rho) = 1$ implies that ρ has to be a density operator. Therefore our convex relaxation assumes the following simple form:

$$\begin{array}{ll} \text{maximize} & \langle A_1 A_1^*, X \rangle \\ \text{subject to} & \operatorname{tr}_{\mathcal{Y}}(X) = \operatorname{tr}_{\mathcal{Y}}(A_0 \rho A_0^*), \\ & X \in \operatorname{Pos}(\mathcal{Y} \otimes Z), \\ & \rho \in D(\mathcal{X}) \end{array} \tag{94}$$

Running this program gives us an upper bound for the optimal value of our QCQP (92). Since the output of idem program corresponds to $\|\Phi\|_1^2$, the SDP (94) gives an upper bound to that value. A closer look on this SDP, however, reveals that it is exactly the SDP for the diamond norm squared ($\|\Phi\|_\diamond^2$) of Φ which has been presented in subsection 3.3.5. Note that this is consistent with what we just said, because $\|\Phi\|_1^2 \leq \|\Phi\|_\diamond^2 \; \forall \Phi \in T(\mathcal{X}, \mathcal{Y})$.

The diamond norm proxy (94) allows us to write down bounds on λ and μ that can be efficiently calculated:

$$\begin{aligned} \mu &= \|\Phi_\mu\|_1 \leq \|\Phi_\mu\|_\diamond, \\ \lambda &= \|\Phi_\lambda\|_1^{-1} \geq \|\Phi_\lambda\|_\diamond^{-1}. \end{aligned}$$

4.3.4 Fidelity based converse bounds

Bounds in the other direction can be obtained via a result from M. Piani and J. Watrous in [9]. They show in Lemma 2 of idem paper that every hermicity preserving trace annihilating superoperator is proportional to the difference of 2 quantum channels. These channels can furthermore be explicitly constructed[13]. Since Φ_1 and Φ_2 are such superoperators, we can find quantum channels $\Psi_\mu^1, \Psi_\mu^2 \in T(\mathcal{X}, \mathcal{Y})$ and $\Psi_\lambda^1, \Psi_\lambda^2 \in T(\mathcal{Y}, \mathcal{X})$, as well as constants c_μ and c_λ such that

$$\begin{aligned} \Phi_\mu &= c_\mu \left(\Psi_\mu^1 - \Psi_\mu^2 \right), \\ \Phi_2 &= c_\lambda \left(\Psi_\lambda^1 - \Psi_\lambda^2 \right). \end{aligned}$$

This allows us to obtain fidelity based bounds by applying the Fuchs-van de Graaf inequalities (9). In order to see this, note that for any X obeying $\|X\|_1 \leq 1$ we have

$$\begin{aligned} \mu &= \|\Phi_\mu\|_1 \geq \|\Phi_\mu(X)\|_1 = c_\mu \|\Psi_\mu^1(X) - \Psi_\mu^2(X)\|_1 \\ &= 2 c_\mu \delta\left(\Psi_\mu^1(X), \Psi_\mu^2(X)\right) \geq 2 c_\mu \left(1 - F\left(\Psi_\mu^1(X), \Psi_\mu^2(X)\right)\right). \end{aligned}$$

Similarly, we can get an analogous result for bounding λ. This reasoning yields the following estimates>

$$\begin{aligned} \mu &\geq 2 c_\mu \left(1 - F\left(\Psi_\mu^1(X), \Psi_\mu^2(X)\right)\right) \quad \text{for any } X \in \operatorname{Herm}(\mathcal{X}) \text{ with } \|X\|_1 \leq 1, , \\ \lambda &\leq \frac{1}{2 c_\lambda} \left(1 - F\left(\Psi_\lambda^1(Y), \Psi_\lambda^2(Y)\right)\right)^{-1} \quad \text{for any } Y \in \operatorname{Herm}(\mathcal{Y}) \text{ with } \|Y\|_1 \leq 1. \end{aligned}$$

[13] In fact it is the Choi representation of these channels that can be explicitly constructed from a Choi representation of the original superoperator.

Note that for any fixed $X \in \mathrm{Herm}(\mathcal{X})$ ($Y \in \mathrm{Herm}(\mathcal{Y})$), the fidelity $F\left(\Psi_\mu^1(X), \Psi_\mu^2(X)\right)$ ($F\left(\Psi_\lambda^1(Y), \Psi_\lambda^2(Y)\right)$) can be efficiently calculated by using, for instance, the SDP[14] presented in subsection 3.3.6. In principle these bounds can be tightened by minimizing the fidelity over all possible states

$$\begin{aligned} \mu &\geq 2c_\mu \left(1 - \min_{\|X\|_1 \leq 1} F\left(\Psi_\mu^1(X), \Psi_\mu^2(X)\right)\right), & (95) \\ \lambda &\leq \frac{1}{2c_\lambda} \left(1 - \min_{\|Y\|_1 \leq 1} F\left(\Psi_\lambda^1(Y), \Psi_\lambda^2(Y)\right)\right)^{-1}. & (96) \end{aligned}$$

However the fidelity is a jointly concave function and therefore minimizing it over the convex set $B(\|.\|_1)$ is computationally hard in general.

4.3.5 Discussion

With this approach we have obtained upper and lower bounds for λ and μ. The diamond norm bounds

$$\begin{aligned} \mu &\leq \|\Phi_\mu\|_\diamond, & (97) \\ \lambda &\geq \|\Phi_\lambda\|_\diamond^{-1} & (98) \end{aligned}$$

are of particular importance, due to the operational significance of λ and μ. Inequality (98) gives a nontrivial lower bound on the worst case promise λ. This bound itself serves as a (weaker) worst case promise. Similarly, inequality (97) gives an upper bound on the optimal performance which can be useful as well. While the upper bound on μ is often likely to be trivial ($\mu \leq 1$), this is never the case for the lower bound on λ ($\lambda > 0$). This is simply because the diamond norm is always finite for sensible superoperators.
Bounds into the other direction are given by (95) and (96). However, they lack the operational significance of their converse counterparts (97) and (98).

The tightness of estimates (97) and (98) is intimately related to the tightness of the inequality $\|\Phi\|_1 \leq \|\Phi\|_\diamond$ for hermicity preserving trace annihilating superoperators $\Phi \in T(\mathcal{X}, \mathcal{Y})$. As already mentioned before, such superoperators correspond to differences of quantum channels $\Psi_1, \Psi_2 \in T(\mathcal{X}, \mathcal{Y})$ ($\Phi = c(\Psi_1 - \Psi_2)$) [9]. Therefore we are actually interested in the tightness of the inequality

$$\|\Psi_1 - \Psi_2\|_1 \leq \|\Psi_1 - \Psi_2\|_\diamond \quad \text{for quantum channels } \Psi_1, \Psi_2. \qquad (99)$$

But this is just the question, whether or not entanglement is useful for the discrimination of quantum channels. If the inequality above is strict, then entanglement really does amplify channel discrimination, while otherwise it does not. While it is easy to construct specific channels Ψ_1, Ψ_2 for which relation (99) is given by an equality, the main result of M. Piani and J. Watrous in [9]

[14] This SDP actually calculates the maximum output fidelity. If we however introduce the SDP constraint $\rho_0 = \rho_1 = X$, the program calculates the required quantity $F(\Phi_0(X), \Phi_1(X))$ instead of $F_{\max}(\Phi_0, \Phi_1)$.

points into the opposite direction. They could show (Corollary 1) that for any entangled state $\rho \in D(\mathcal{X} \otimes \mathcal{Z})$ there exist channels $\Xi_1, \Xi_2 \in T(\mathcal{X}, \mathcal{Y})$ such that

$$\left\| \left(\Xi_1 \otimes \mathbb{I}_{L(\mathcal{Z})} \right)(\rho) - \left(\Xi_2 \otimes \mathbb{I}_{L(\mathcal{Z})} \right)(\rho) \right\|_1 > \| \Xi_1 - \Xi_2 \|_1.$$

Hence, $\|\Xi_1 - \Xi_2\|_\diamond > \|\Xi_1 - \Xi_2\|_1$ for the occuring channels. This indicates that for random entanglement breaking channels Ψ_1, Ψ_2, inequality (99) is likely to be strict. However this conjecture seems difficult to prove and the authors are not aware of any proof attempt in the literature.

Finally we want to point out that the convex relaxation of our algorithm for calculating $\|\Phi\|_1$ is given by an algorithm for the corresponding diamond norm $\|\Phi\|_\diamond$. This coincides with the folk knowledge that the diamond norm is a stabilized version of the induced 1-norm. It would be interesting to explore, whether this relation is fundamental, or just an artifact of the particular algorithm we have used.

5 Conclusion and Outlook

In this work we have focused on the POVM norm constants λ and μ. These constants were introduced by W. Matthews, S. Wehner and A. Winter [4] in the field of state discrimination. They allow for comparing the performance of an actual informationally complete POVM measurement $\{M_k\}_{k=1}^n$ on a m-dimensional operator space $\mathrm{Herm}(\mathcal{X})$ to the ideal measurement that is given by the union of all possible POVMs. This attests operational significance to these numbers. In this thesis we have introduced two methods for computing or bounding such POVM norm constants.

The first method, dubbed *polytope approach*, is of geometric nature. It obtains λ (or its non-traceless analogue $\tilde{\lambda}$) via maximizing a convex function over a convex polytope. Such a maximization corresponds to checking the function's value at all extreme points (vertices) of the considered polytope. Hence, the efficiency of the polytope algorithm crucially depends on the number of vertices l'. This number is potentially large and conjectured to scale at most exponentially in $(n - m)$. Proving this conjecture and explicitly constructing corresponding intersection polytopes seems challenging and would be very interesting on its own. Due to the scaling properties of the number of vertices, our approach is likely to be computationally hard for $m \ll n$.

However, our approach is particularly well suited for exactly informationally complete POVMs $\{M_k\}_{k=1}^n$ over $\mathbb{C}^d$ (i.e. $M_k \in \mathrm{Pos}\left(\mathbb{C}^d\right)$ for each $k = 1, \ldots, n$) which obey $n = m = d^2$. In this special case the polytope admits at most $2n(n-1)$ vertices which are furthermore known explicitly. Obtaining λ (or $\tilde{\lambda}$) can thus be done efficiently by checking the objective function's value at each such vertex. We considered arbitrary SIC POVMs as a special case of such exactly informationally complete measurements. Due to their high degree of symmetry we could calculate $\lambda = \frac{1}{d}$ (and $\tilde{\lambda} = \frac{1}{2d-1}$) analytically. This tightens the previously known bound $\frac{1}{2}\frac{1}{d+1} \leq \lambda \leq \frac{1}{d}$ from [4]. The polytope approach is in general not suited well for POVMs that contain a lot of redundancy (i.e.:

$n \gg m$). In such situations, the considered polytope can have exponentially many vertices. This makes checking the objective function's value at each vertex computationally hard. However, a relaxed version of the polytope approach (see subsection 4.2.4) allows for obtaining computationally cheap upper and lower bounds on λ (and $\tilde{\lambda}$). The worst case accuracy of such a lower bound is given by $\frac{1}{\sqrt{n}}$. Note that in this work we have focused on the most general case and have not considered possible additional structure of the POVMs. We believe, for instance, that possible POVM symmetries induce restrictions on the polytope of interest. These restrictions could substantially reduce the polytope's number of vertices and considerable speed up our algorithm. Another way of circumvening the infavourable case $n \gg m$ is to look for clever ways of redundancy removal. By redundancy removal we mean procedures that convert an arbitrary informationally complete POVM $\{M_k\}_{k=1}^n$ into an exactly informationally complete one $\left\{M_k^{'}\right\}_{k=1}^{m}$. If such a procedure conserves λ (in the sense that $(1-c_1)\lambda^{'} \leq \lambda \leq (1+c_2)\lambda^{'}$ for $c_1, c_2 > 0$ small), it would allow us to calculate $\lambda^{'}$ instead of λ. This can then of course be done efficiently. Exploiting symmetries and looking for redundancy removal procedures that conserve λ constitute interesting follow-up projects.

Our second method, the ***diamond approach***, yields upper and lower bounds on both POVM norm constants λ and μ. The upper bounds on μ and $\frac{1}{\lambda}$ (i.e. the lower bound on λ) are much more relevant and obtained via computing the diamond norm of certain superoperators. We presented an explicit construction of these superoperators that depends solely on the POVM of interest. Constructing this superoperator and then evaluating its diamond norm via an SDP allows for computing these bounds efficiently. However, the accuracy of these bounds is not completely understood yet. Interestingly, this precision is closely related to the question of how useful entanglement is for distinguishing arbitrary quantum channels. To our knowledge, no full answer to this question is known yet. It would be of independent interest to further investigate this problem. Finally, we mention that the less important converse bounds can be computed efficiently via a similar procedure that uses the fidelity.

Acknowledgements I want to thank Prof. Matthias Christandl for proposing the topic of my thesis and contributing many useful ideas. Special thanks is to Dr. Frédéric Dupont-Dupuis for his supervision and dedicated guidance throughout the whole project.
Furthermore, I would like to thank Prof. David Gross, Michael Walter and Andreas Hermann for insightful discussions.
I also want to thank David Hasselhoff for many inspiring moments.
Financial Support from the Swiss National Science Foundation and the Swiss National Center of Competence in Research "Quantum Science and Technology" is gratefully acknowledged.

Appendix

Norm constants for a 1-Qubit POVM

In this appendix chapter we present some example calculations for 1-qubit systems, for which we use Bloch sphere representation. Any density operator $\rho \in D\left(\mathbb{C}^2\right)$ is represented by a vector $\vec{r} \in \mathbb{R}^3$ via

$$\rho = \frac{1}{2}\left(\mathbb{I} + \vec{r}.\vec{\sigma}\right), \tag{100}$$

where $\vec{\sigma} = \left(\sigma_x, \sigma_y, \sigma_z\right)^T$ and $\|\vec{r}\|_{l^2} \leq 1$. The operators $\sigma_x, \sigma_y, \sigma_z$ denote the Pauli matrices[15].

In the first subsection we calculate the POVM-norm constants λ and μ for a very simple informationally complete POVM.

The POVM

A simple POVM for one Qubit is given by the following selection of matrices

$$\left(M_k\right)_{k=1}^{6} := \left\{\frac{1}{3}|0\rangle\langle 0|,\ \frac{1}{3}|1\rangle\langle 1|,\ \frac{1}{3}|+\rangle\langle +|,\ \frac{1}{3}|-\rangle\langle -|,\ \frac{1}{3}|\circlearrowright\rangle\langle\circlearrowright|,\ \frac{1}{3}|\circlearrowleft\rangle\langle\circlearrowleft|\right\}. \tag{101}$$

Here we have used the following convention

$$\begin{aligned} |+\rangle &:= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \qquad |-\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \\ |\circlearrowright\rangle &:= \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right) \qquad |\circlearrowleft\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right). \end{aligned}$$

If we agree on working in the $|0\rangle, |1\rangle$-basis, we obtain the following matrix expressions for our POVM elements:

$$\begin{aligned} M_1 &= \frac{1}{3}|0\rangle\langle 0| = \frac{1}{3}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, & M_2 &= \frac{1}{3}|1\rangle\langle 1| = \frac{1}{3}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \\ M_3 &= \frac{1}{3}|+\rangle\langle +| = \frac{1}{6}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, & M_4 &= \frac{1}{3}|-\rangle\langle -| = \frac{1}{6}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \\ M_5 &= \frac{1}{3}|\circlearrowright\rangle\langle\circlearrowright| = \frac{1}{6}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} & M_6 &= \frac{1}{3}|\circlearrowright\rangle\langle\circlearrowright| = \frac{1}{6}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}. \end{aligned}$$

Note that this collection indeed fulfills the defining property of a POVM:

$$\sum_{k=1}^{6} M_k = \left(M_1 + M_2\right) + \left(M_3 + M_4\right) + \left(M_5 + M_6\right) = \frac{1}{3}\mathbb{I}_2 + \frac{1}{3}\mathbb{I}_2 + \frac{1}{3}\mathbb{I}_2 = \mathbb{I}_2.$$

[15] i.e.: $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

It furthermore contains a basis of all 2×2-matrices, which makes it informationally complete. In order to see this, we point out that

$$3\left(M_3 - M_4\right) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad 3i\left(M_5 - M_6\right) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

It is obvious that the collection $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$ forms a basis of $M_2\left(\mathbb{C}^2\right)$.

A straightforward calculation yields the following overlaps between our POVM elements and the Pauli matrices

$$\begin{aligned} \mathrm{tr}\left\{\sigma_i M_1\right\} &= \frac{1}{3}\delta_i^z, & \mathrm{tr}\left\{\sigma_i M_2\right\} &= -\frac{1}{3}\delta_i^z, \\ \mathrm{tr}\left\{\sigma_i M_3\right\} &= \frac{1}{3}\delta_i^x, & \mathrm{tr}\left\{\sigma_i M_4\right\} &= -\frac{1}{3}\delta_i^x, \\ \mathrm{tr}\left\{\sigma_i M_5\right\} &= \frac{1}{3}\delta_i^y, & \mathrm{tr}\left\{\sigma_i M_6\right\} &= -\frac{1}{3}\delta_i^y. \end{aligned}$$

Calculating the POVM-norm constants

Note that the Bloch sphere representation (100) for differences of qubits $\rho - \sigma$ amounts to

$$\rho - \tau = \frac{1}{2}\left(\vec{r} - \vec{t}\right)\vec{\sigma} =: \frac{1}{2}\vec{d}\vec{\sigma},$$

where $\vec{d} = \vec{d}\left(\vec{r}, \vec{t}\right)$ denotes the corresponding difference vector. This representation assures tracelessness. We can insert this expression into our measurement channel and obtain

$$\begin{aligned} \mathcal{M}\left(\vec{d}\right) &= \sum_{k=1}^{n} |k\rangle\langle k|\ \mathrm{tr}\left\{\frac{1}{2}\vec{d}\vec{\sigma}M_k\right\} \\ &= \frac{1}{2}\sum_{k=1}^{n} |k\rangle\langle k|\ d^i \mathrm{tr}\left\{\sigma_i M_k\right\} \\ &= \frac{1}{2}|1\rangle\langle 1| d^i \mathrm{tr}\left\{\sigma_i M_1\right\} + \frac{1}{2}|2\rangle\langle 2| d^i \mathrm{tr}\left\{\sigma_i M_2\right\} \\ &+ \frac{1}{2}|3\rangle\langle 3| d^i \mathrm{tr}\left\{\sigma_i M_3\right\} + \frac{1}{2}|4\rangle\langle 4| d^i \mathrm{tr}\left\{\sigma_i M_4\right\} \\ &+ \frac{1}{2}|5\rangle\langle 5| d^i \mathrm{tr}\left\{\sigma_i M_5\right\} + \frac{1}{2}|6\rangle\langle 6| d^i \mathrm{tr}\left\{\sigma_i M_6\right\} \\ &= \frac{1}{6}\left\{d_z\left(|1\rangle\langle 1| - |2\rangle\langle 2\right) + d_x\left(|3\rangle\langle 3| - |4\rangle\langle 4|\right) + d_y\left(|5\rangle\langle 5 - |6\rangle\langle 6|\right)\right\}. \end{aligned}$$

From this we can directly infer the corresponding trace-norm value

$$\|\mathcal{M}\left(\rho - \tau\right)\|_1 = \frac{1}{6}\left(2|d_z| + 2|d_x| + 2|d_y|\right) = \frac{1}{3}\|\vec{d}\|_{l_1}.$$

The original trace distance amounts to

$$\|\rho-\tau\|_1 \quad = \quad \|\frac{1}{2}\vec{d}\vec{\sigma}\|_1 = |\lambda_1| + |\lambda_2|,$$

where λ_i $i = 1, 2$ denote the eigenvalues of $\frac{1}{2}\vec{d}\vec{\sigma}$. We can calculate the eigenvalues of $\frac{1}{2}\vec{d}\vec{\sigma}$ via the standard procedure. Note that

$$\begin{aligned} \frac{1}{2}\vec{d}\vec{\sigma} &= \frac{1}{2}\left\{ d_x \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + d_y \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + d_z \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \\ &= \frac{1}{2}\begin{pmatrix} d_z & d_x - i d_z \\ d_x + i d_z & -d_z \end{pmatrix}. \end{aligned}$$

The characteristic polynomial of this matrix amounts to

$$\begin{aligned} p(\lambda) &= \left(\frac{1}{2}d_z - \lambda\right)\left(-\frac{1}{2}d_z - \lambda\right) - \frac{1}{2}\left(d_x - i d_z\right)\frac{1}{2}\left(d_x + i d_z\right) \\ &= \left(\lambda^2 - \frac{1}{4}d_z^2 - \frac{1}{4}d_z^2 - \frac{1}{4}d_z^2\right). \end{aligned}$$

Therefore:

$$\lambda_{1,2} = \pm\frac{1}{2}\sqrt{d_x^2 + d_y^2 + d_z^2} = \pm\frac{1}{2}\|\vec{d}\|_{l_2}.$$

This allows us to calculate the actual distance between ρ and τ:

$$\|\rho-\tau\|_1 = |\lambda_1| + |\lambda_2| = \|\vec{d}\|_2. \tag{102}$$

Now we are ready to compare the two relevant norms

$$\begin{aligned} \|\rho-\tau\|_1 &= \|\vec{d}\|_2 \quad \text{and} \\ \|\mathcal{M}\left(\rho-\tau\right)\|_1 &= \frac{1}{3}\|\vec{d}\|_1. \end{aligned}$$

We use the basic fact that in n dimensions we have for arbitrary $x \in \mathbb{R}^n$:

$$\|x\|_1 = \langle \operatorname{sgn}(x), x \rangle \leq \|\operatorname{sgn}(x)\|_2 \|x\|_2 = \sqrt{n}\|x\|_2,$$

which is due to Cauchy-Schwarz. Note that this inequality is actually tight[16] for $S^{n-1} \subset \mathbb{R}^n$. In 3 dimensions this indeed assures

$$\|\mathcal{M}\left(\rho-\tau\right)\|_1 = \frac{1}{3}\|\vec{d}\|_1 \leq \frac{1}{\sqrt{3}}\|\vec{d}\|_2 = \frac{1}{\sqrt{3}}\|\rho-\tau\|_1, \tag{103}$$

Using another well known and tight[17] inequality $\|x\|_2 \leq \|x\|_1$, we can also go into the other direction:

$$\|\rho-\tau\|_1 = \|\vec{d}\|_2 \leq \|\vec{d}\|_1 = \frac{3}{3}\|\vec{d}\|_1 = 3\|\mathcal{M}\left(\rho-\tau\right)\|_1. \tag{104}$$

[16] Take for example $x = \frac{1}{\sqrt{n}}\left(1, \ldots, 1\right)^T$. Then $\|x\|_1 = \sqrt{d}$ and $\|x\|_2 = 1$.

[17] Take for example $x = \left(1, 0, \ldots, 0\right)^T$, then $\|x\|_2 = 1 = \|x\|_1$.

Combining (103) and (104) yields

$$\frac{1}{3}\|\rho-\tau\|_1 \leq \|\mathcal{M}\left(\rho-\tau\right)\|_1 \leq \frac{1}{\sqrt{3}}\|\rho-\tau\|_1. \tag{105}$$

Therefore we have $\mu = \frac{1}{\sqrt{3}}$ and $\lambda = \frac{1}{3}$.

A slight generalization of the POVM

As a slight generalization we consider strict convex combinations of the 3 (mutually unbiased) bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ and $\{|\circlearrowright\rangle, |\circlearrowleft\rangle\}$. By this we mean that we introduce three constants $\alpha, \beta, \gamma \in]0,1[$ such that $\alpha+\beta+\gamma = 1$ and modify (101) in the following way:

$$\left(M_k\left(\alpha,\beta,\gamma\right)\right)_{k=1}^{6} := \left\{\alpha|0\rangle\langle 0|,\ \alpha|1\rangle\langle 1|,\ \beta|+\rangle\langle +|,\ \beta|-\rangle\langle -|,\ \gamma|\circlearrowright\rangle\langle\circlearrowright|,\ \gamma|\circlearrowleft\rangle\langle\circlearrowleft|\right\}.$$

This POVM is still informationally complete, because $\alpha, \beta, \gamma > 0$. However, the trace relations with the Pauli matrices turn into:

$$\begin{aligned} \operatorname{tr}\{\sigma_i M_1\} &= \alpha\delta_i^z, \qquad \operatorname{tr}\{\sigma_i M_2\} = -\alpha\delta_i^z, \\ \operatorname{tr}\{\sigma_i M_3\} &= \beta\delta_i^x, \qquad \operatorname{tr}\{\sigma_i M_4\} = -\beta\delta_i^x, \\ \operatorname{tr}\{\sigma_i M_5\} &= \gamma\delta_i^y, \qquad \operatorname{tr}\{\sigma_i M_6\} = -\gamma\delta_i^y. \end{aligned}$$

Following the same steps as before, we get

$$\begin{aligned} \mathcal{M}\left(\vec{d}\right) &= \sum_{k=1}^{n} |k\rangle\langle k| \operatorname{tr}\left\{\frac{1}{2}\vec{d}\vec{\sigma}M_k\right\} \\ &= \frac{1}{2}\sum_{k=1}^{n} |k\rangle\langle k|\ d^i \operatorname{tr}\{\sigma_i M_k\} \\ &= \frac{1}{2}|1\rangle\langle 1| d^i \operatorname{tr}\{\sigma_i M_1\} + \frac{1}{2}|2\rangle\langle 2| d^i \operatorname{tr}\{\sigma_i M_2\} \\ &+ \frac{1}{2}|3\rangle\langle 3| d^i \operatorname{tr}\{\sigma_i M_3\} + \frac{1}{2}|4\rangle\langle 4| d^i \operatorname{tr}\{\sigma_i M_4\} \\ &+ \frac{1}{2}|5\rangle\langle 5| d^i \operatorname{tr}\{\sigma_i M_5\} + \frac{1}{2}|6\rangle\langle 6| d^i \operatorname{tr}\{\sigma_i M_6\} \\ &= \frac{1}{2}\left\{\alpha d_z\left(|1\rangle\langle 1| - |2\rangle\langle 2\right) + \beta d_x\left(|3\rangle\langle 3| - |4\rangle\langle 4|\right) + \gamma d_y\left(|5\rangle\langle 5 - |6\rangle\langle 6|\right)\right\}, \end{aligned}$$

which results in the following expression:

$$\|\mathcal{M}\left(\rho-\tau\right)\|_1 = \frac{1}{2}\left(2\alpha|d_z| + 2\beta|d_x| + 2\gamma|d_y|\right) = \beta|d_x| + \gamma|d_y| + \alpha|d_z|.$$

Therefore we need to compare the following quantities:

$$\begin{aligned} \|\rho-\tau\|_1 &= \|\vec{d}\|_2, \\ \|\mathcal{M}\left(\rho-\tau\right)\|_1 &= \beta|d_x| + \gamma|d_y| + \alpha|d_z|. \end{aligned}$$

Note that

$$\|\mathcal{M}\left(\rho-\tau\right)\|_1 \geq \min\left(\alpha,\beta,\gamma\right)\|\vec{d}\|_1 \geq \min\left(\alpha,\beta,\gamma\right)\|\vec{d}\|_2 = \min\left(\alpha,\beta,\gamma\right)\|\rho-\tau\|_1,$$

which is tight. Hence, we have already found one direction of our bound. For obtaining the other direction, we proceed in a similar way:

$$\|\mathcal{M}\left(\rho-\tau\right)\|_1 \leq \max\left(\alpha,\beta,\gamma\right)\|\vec{d}\|_1 \leq \sqrt{3}\max\left(\alpha,\beta,\gamma\right)\|\vec{d}\|_2 = \sqrt{3}\max\left(\alpha,\beta,\gamma\right)\|\rho-\tau\|_1, \tag{106}$$

which is now not tight anymore[18]. Therefore we have found the following sandwich that generalizes (105):

$$\min\left(\alpha,\beta,\gamma\right)\|\rho-\tau\|_1 \leq \|\mathcal{M}\left(\rho-\tau\right)\|_1 \leq \sqrt{3}\max\left(\alpha,\beta,\gamma\right)\|\rho-\tau\|_1. \tag{107}$$

Note that (107) indeed contains (105) as a special case for $\alpha=\beta=\gamma=\frac{1}{3}$. For this choice of parameters we obtain a tight[19] sandwich.

[18] Assume $\max\left(\alpha,\beta,\gamma\right)=\beta$, then the first inequality is tight for $\vec{d}=(1,0,0)^T$, whereas the second inequality is tight for $\vec{d}=\frac{1}{\sqrt{3}}\left(1,1,1\right)^T$.

[19] Note that the first inequality in (106) becomes an equality for $\alpha=\beta=\gamma$.

References

[1] Plato, Politeia (the Republic), 380 BC

[2] Punya Misha's web page, http://punya.educ.msu.edu/2010/09/03/abc-triplet-ambigram/

[3] C.W. Helstrom, Quantum Detection and Estimation Theory, Academic Press, New York, (1976)

[4] W. Matthews, S. Wehner, A. Winter, "Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding", 2008

[5] M. Christandl, R. Renner, Reliable quantum state tomography, 2011

[6] C. Schütte-Nütgen, Construction of Confidence Regions in Quantum Tomography, Master thesis (ETH Zürich), 2012

[7] D. Reeb, M.J. Kastoryano, M.M. Wolf, Hilbert's projective metric in quantum information theory, Journal of mathematical physics 52, 082201 (2011)

[8] J. Watrous, Notes on super-operator norms induced by Schatten norms, 2004

[9] M. Piani, J. Watrous, All entangled states are useful for channel discrimination

[10] J. Watrous, Semidefinite programs for completely bounded norms, 2009

[11] J. Watrous, Theory of Quantum Information (lecture notes 2011), www.cs.uwaterloo.ca/∼watrous/CS766/

[12] M. Thomamichel, A Framework for Non-Asymptotic Quantum Information Theory, PhD thesis (ETH Zürich) 2012

[13] A. S. Holevo, Quantum coding theorems, Russian Math. Surveys, 53, 1295-1331 (1999)

[14] C. King, Maximal p-norms of entanglement breaking channels, 2008

[15] J. de Pillis, Linear transformations which preserve Hermitian and positive semidefinite operators, Pacific Journal of Mathematics, 23(1):129-137.1967

[16] A Jamiolkowski, Linear transformations which preserve trace and positive semidefiniteness of operators, Reports on Mathematical Physics, 3(4):275-278, 1972

[17] M. Choi, Completely positive linear maps on complex matrices. Linear Algebra and its Applications, 10(3): 285-290, 1975

[18] A. Barvinok, A course in convexity, American Mathematical Society, 2002

[19] S. Boyd, L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004

[20] HSM Coxeter, Regular Polytopes, 3rd ed., Dover, New York, 1973

[21] G. Ziegler, Lectures on Polytopes, Graduate Texts in Mathematics 152, Springer Verlag New York, 1995

[22] F. Goodman, Algebra: Abstract and Concrete, www.math.uiowa.edu/∼goodman/algebrabook.dir/images.html

[23] A. d'Aspremont, S. Boyd, Relaxations and Randomized Methods for Nonconvex QCQPs, 2003

[24] X. Zheng, X. Ling Sun, D. Li, Convex relaxations for noconvex quadratically constrained quadratic programming: matrix cone decomposition and polyhedral approximation, 2011

[25] J. Gallier, The Schur Complement and Symmetric Positive Semidefinite (and Definite) Matrices, 2010

[26] D. Avis, K. Fukuda, A Pivoting Algorithm for Convex Hulss and Vertex Enumeration of Arrangements an Polyhedra, Discrete comput Geom 8:295-313 (1992)

[27] K. Fukuda, Frequently Asked Questions in Polyhedral Computation, 2004

[28] K. Fukuda, Th. Liebling, C. Lütolf, Extended convex hull, Proceedings of the 12th Canadian Conference on Computational Geometry, 57-63, 2000

[29] H. Tiwary, On the Hardness of Computing Intersection, Union and Minkowski Sum of Polytopes, Discrete Comput Geom 40: 469-479, 2008

[30] V. Milman, G. Schechtman, Asymptotic theory of finite-dimensional normed spaces, Springer-Verlag, Berlin, 1986

[31] J. Lee, the Pseudorandom Subspace Problem, blog entry in tcs math 2008, http://tcsmath.wordpress.com/2008/05/04/the-pseudorandom-subspace-problem/

[32] J. Renes, R. Blume-Kohout, A. Scott, C. Caves, Symmetric informationally complete measurements, 2003