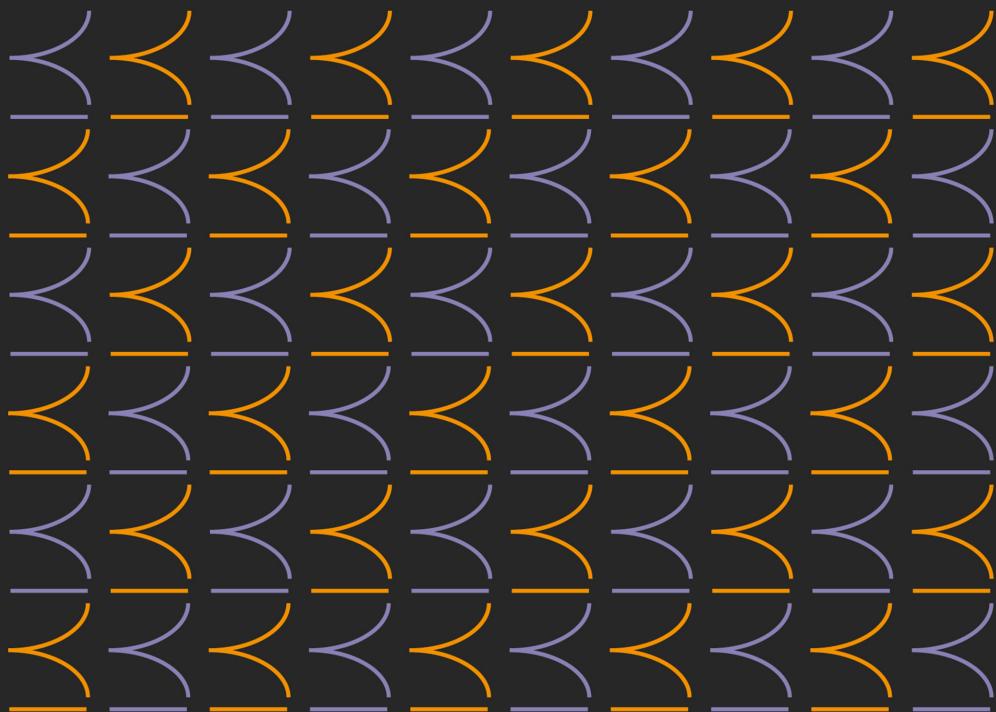


IOP Series in Quantum Technology

# Semidefinite Programming in Quantum Information Science

**Paul Skrzypczyk**  
**Daniel Cavalcanti**



# Semidefinite Programming in Quantum Information Science

Online at: <https://doi.org/10.1088/978-0-7503-3343-6>

# IOP Series in Quantum Technology

**Series Editor:** **Barry Garraway** (School of Mathematical and Physical Sciences, University of Sussex, UK), **Barry Sanders** (Institute for Quantum Science and Technology, University of Calgary, Canada), and **Lincoln Carr** (Quantum Engineering Program, Colorado School of Mines, USA)

## About the series

The IOP Series in Quantum Technology is dedicated to bringing together the most up to date texts and reference books from across the emerging field of quantum science and its technological applications. Prepared by leading experts, the series is intended for graduate students and researchers either already working in or intending to enter the field. The series seeks (but is not restricted to) publications in the following topics:

- Quantum biology
- Quantum communication
- Quantum computation
- Quantum control
- Quantum cryptography
- Quantum engineering
- Quantum machine learning and intelligence
- Quantum materials
- Quantum metrology
- Quantum optics
- Quantum sensing
- Quantum simulation
- Quantum software, algorithms and code
- Quantum thermodynamics
- Hybrid quantum systems

A full list of titles published in this series can be found here: <https://iopscience.iop.org/bookListInfo/iop-series-in-quantum-technology>

# Semidefinite Programming in Quantum Information Science

**Paul Skrzypczyk**

*School of Physics, University of Bristol, Bristol, UK*

**Daniel Cavalcanti**

*Algorithmiq Ltd, Helsinki, Finland*

**IOP** Publishing, Bristol, UK

© IOP Publishing Ltd 2023

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, or as expressly permitted by law or under terms agreed with the appropriate rights organization. Multiple copying is permitted in accordance with the terms of licences issued by the Copyright Licensing Agency, the Copyright Clearance Centre and other reproduction rights organizations.

Permission to make use of IOP Publishing content other than as set out above may be sought at [permissions@ioppublishing.org](mailto:permissions@ioppublishing.org).

Paul Skrzypczyk and Daniel Cavalcanti have asserted their right to be identified as the authors of this work in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

ISBN 978-0-7503-3343-6 (ebook)

ISBN 978-0-7503-3341-2 (print)

ISBN 978-0-7503-3344-3 (myPrint)

ISBN 978-0-7503-3342-9 (mobi)

DOI 10.1088/978-0-7503-3343-6

Version: 20230301

IOP ebooks

British Library Cataloguing-in-Publication Data: A catalogue record for this book is available from the British Library.

Published by IOP Publishing, wholly owned by The Institute of Physics, London

IOP Publishing, No.2 The Distillery, Glassfields, Avon Street, Bristol, BS2 0GR, UK

US Office: IOP Publishing, Inc., 190 North Independence Mall West, Suite 601, Philadelphia, PA 19106, USA

Supplementary material is available at <https://github.com/paulskrzypczyk/SDPBook>.

# Contents

<b>Preface</b>	viii
<b>Author biographies</b>	ix
<b>About this book</b>	x

## Part I The fundamentals

<b>1 Linear programming</b>	<b>1-1</b>
1.1 The basics	1-1
1.1.1 Feasibility	1-6
1.2 Geometric interpretation	1-11
1.2.1 Equality constraints	1-11
1.2.2 Inequality constraints	1-11
1.2.3 The feasible set	1-11
1.2.4 The objective function	1-14
1.3 Duality	1-18
1.4 Slack variables	1-22
1.5 Weak and strong duality	1-23
1.6 Concluding remarks	1-25
1.7 Advanced topics	1-25
1.7.1 Complementary slackness	1-26
1.7.2 Dual form of $\ell_1$ and $\ell_\infty$ norms	1-28
1.8 Further reading	1-31
<b>2 Semidefinite programming</b>	<b>2-1</b>
2.1 Primal semidefinite programs	2-1
2.2 Duality	2-6
2.3 Weak and strong duality	2-10
2.4 Complementary slackness	2-14
2.5 Linear programs as special instances of semidefinite programs	2-16
2.6 Concluding remarks	2-18
2.7 Further reading	2-18

## Part II Semidefinite programming in quantum information science

<b>3</b>	<b>Quantum states</b>	<b>3-1</b>
3.1	Quantum state estimation	3-2
3.1.1	Trace distance estimation	3-3
3.1.2	Fidelity estimation	3-5
3.1.3	Finite statistics	3-7
3.1.4	Relaxing the feasibility problem	3-8
3.1.5	Certificate of infeasibility	3-10
3.1.6	Geometrical interpretation	3-13
3.1.7	Property estimation	3-16
3.2	The quantum marginal problem	3-17
3.3	Concluding remarks	3-21
3.4	Further reading	3-22
3.5	Advanced topics	3-22
3.5.1	The fidelity SDP	3-22
<b>4</b>	<b>Quantum measurements</b>	<b>4-1</b>
4.1	Quantum measurement estimation	4-1
4.2	Quantum state discrimination I	4-4
4.2.1	Minimum-error quantum state discrimination	4-5
4.2.2	Binary state discrimination	4-6
4.2.3	Optimality conditions	4-8
4.2.4	Unambiguous quantum state discrimination	4-11
4.3	Quantum state discrimination II	4-12
4.3.1	Transforming the non-linear problem into a linear one	4-17
4.3.2	Generalised robustness of measurement informativeness	4-20
4.3.3	Structure of the optimal ensemble and noise measurement	4-24
4.4	Concluding remarks	4-26
4.5	Further reading	4-27
4.6	Advanced topics	4-27
4.6.1	Unambiguous quantum state discrimination revisited	4-27
<b>5</b>	<b>Quantum entanglement</b>	<b>5-1</b>
5.1	Entanglement of pure and mixed states	5-1
5.2	The positive-partial-transpose criterion	5-2
5.3	Entanglement negativity	5-5

5.4	Random robustness of entanglement and SDP relaxations	5-11
5.5	$k$ -symmetric extensions	5-15
5.6	Concluding remarks	5-21
5.7	Further reading	5-22
5.8	Advanced topics	5-22
	5.8.1 Entanglement witnesses from $k$ -symmetric extensions	5-22
<b>6</b>	<b>Measurement incompatibility</b>	<b>6-1</b>
6.1	Joint measurability as an SDP	6-1
6.2	Two dichotomic measurements	6-4
6.3	Concluding remarks	6-9
6.4	Further reading	6-9
6.5	Advanced topics	6-9
	6.5.1 Measurement incompatibility and quantum nonlocality	6-9
<b>7</b>	<b>Quantum channels</b>	<b>7-1</b>
7.1	The Choi–Jamiołkowski isomorphism	7-1
7.2	Channel estimation	7-4
7.3	The diamond norm and channel discrimination	7-6
7.4	The conditional min-entropy and the singlet fidelity	7-10
7.5	Concluding remarks	7-19
7.6	Further reading	7-19
7.7	Advanced topics	7-19

# Preface

We can safely say that learning semidefinite programming was a turning point in both of our careers. It all started in 2013, when we both joined Prof. Antonio Acín's group at ICFO—The Institute of Photonic Sciences (Barcelona) to conduct our postdoctoral research. At that time we became interested in the problem of characterising quantum steering, a form of quantum correlations that were first noticed by Schrödinger in response to Einstein, Podolsky and Rosen's famous 1935 paper. We suspected that there was more to discover about quantum steering, and the role it can play in quantum information science. It was then, during the traditional Quantum Information Conference '13, held in the beautiful mountain village of Benasque (Spain), that Miguel Navascués (now a group leader at the University of Vienna) mentioned that steering could be studied using semidefinite programming. We immediately started digging into this idea and, a few months later, we published our first paper (also in collaboration with Miguel) showing how to use semidefinite programming in the quantification of steering. Since then, we have both been using semidefinite programming directly to achieve results in quantum information and foundations, or indirectly to test assumptions, to the point that using this technique has become an obsession. In fact, this is the main reason why we decided to write this book: semidefinite programming has helped us tremendously, and we are sure that it will help other researchers too.

We also have to mention the push we got from the VII Paraty Quantum Information School in 2019, where one of us was invited to give a mini-course on the topic of this book. During this event we saw a big interest from students on the topic, and realised there was a lack of a concise and coherent source of information about it, that could appeal to theorist or experimentalist, mathematician or physicist, and all those in between.

Because of this, we would like to thank Antonio Acín for providing us with a relaxed and inspiring collaborative environment in his group. We would also like to thank Miguel Navascués, and everyone involved in the organisation of the Benasque Quantum Information Conference as well as the organisers and students of the VII Paraty Quantum Information School. We also thank our numerous colleagues who, for so many times, have helped us to better understand semidefinite programming. In particular Marco T Quintino, Dennis Rosset, Jean D Bancal, Valerio Scarani, Marco Piani, Ashley Montanaro, Tony Short, and Sandu Popescu. Finally, we would like to thank IOP Publishing, and in particular John Navas, for giving us the opportunity to write this book.

# Author biographies

## Paul Skrzypczyk



Paul Skrzypczyk is currently an Associate Professor and Royal Society University Research Fellow at the University of Bristol in the School of Physics. He obtained his PhD in Theoretical Physics from the University of Bristol in 2011, under the supervision of Professor Sandu Popescu, with his PhD studies focusing on quantum nonlocality and quantum thermodynamics. He carried out postdoctoral research at the University of Cambridge, and ICFO—The Institute for Photonic Sciences, before returning to Bristol in 2015. In 2016 he was awarded a Royal Society University Research Fellowship, and became a lecturer in 2018 and an Associate Professor in 2022. Paul’s research interest span many areas of quantum information and quantum foundations, ranging from quantum nonlocal effects, such as Bell nonlocality, quantum steering and quantum teleportation, to quantum measurements and measurement incompatibility, to quantum thermodynamics. Convex geometry, semidefinite programming and convex optimisation have been the primary mathematical tools used in his research over the years.

## Daniel Cavalcanti



Daniel Cavalcanti is currently a senior researcher at Algoritmique Ltd. He obtained a PhD in Theoretical Physics at ICFO—Institute of Photonic Sciences in 2008 on the topics of entanglement and characterisation of quantum correlations. After a short postdoc at ICFO in 2009, he joined the Centre for Quantum Technology (Singapore) in 2010, first as a postdoc in Professor Valerio Scarani’s group, and soon as an independent researcher. In 2013 he returned to ICFO, where he stayed until 2021 on a Ramón y Cajal grant. Daniel’s research has focused on quantum foundations, quantum correlations, quantum communication and, more recently, quantum computation. Daniel also holds a master’s degree in graphic design and runs Bitflow, a graphic design studio dedicated to science and technology related projects.

# About this book

Semidefinite programming (SDP<sup>1</sup>) is a type of optimisation problem with vast applications in physics, engineering, combinatorial optimisation, and many other fields. In this book we are interested in applications of semidefinite programming in the field of quantum information. It turns out to be pretty natural that many problems in quantum mechanics and quantum information can be cast as SDPs, because the mathematical description of quantum states and quantum measurements in terms of positive semidefinite operators fit naturally in the SDP framework. Thus, although here we will mostly focus on quantum information, the present book can also be relevant when addressing other problems in quantum physics.

From a practical point of view, there are two main reasons to study SDPs. First, once a problem is recognised as an SDP, there is a theoretical machinery that can be used to solve the problem or, at least, obtain bounds on its solution. Second, there are plenty of efficient computer algorithms and modelling languages for solving SDPs, such as **CVX**, **CVXOPT**, **CVXPY**, **MOSEK** and **YALMIP**, allowing us to numerically solve SDPs involving relatively big matrices with today's standard laptop computers. As a starting point for performing numerical calculations of SDPs we recommend in particular the **CVX** and **CVXPY** modelling systems for constructing and solving convex optimisation problems (of which SDPs are a subclass) that can be implemented in **Matlab** and **Python** respectively. This book will focus exclusively on the theoretical machinery of SDPs. However, to accompany it, we have set up a repository at <https://github.com/paulskrzypczyk/SDPBook>, which contains a small number of example codes, covering some of the SDPs studied in this book.

The structure of this book is the following. It is split into two parts. Part I is devoted to the description of semidefinite programming, focusing on its main aspects. It starts with a simpler subclass of optimisation problems called *linear programs* (chapter 1) and then moves on to the main description of SDPs (chapter 2). In these two chapters we will also set up the notation, nomenclature and basic definitions and concepts that will be used throughout the book. Then, Part II is devoted to particular problems from across the realm of quantum information science that can be tackled with the help of semidefinite programming. The list of problems we consider here is by no means exhaustive. Nonetheless, it is important to explain a little about the choice of problems presented. First, we wanted to cover a wide range of problems in quantum information. In this regard, you will find chapters related to quantum states, measurements, entanglement and channels. Second, we have chosen problems specifically that allow us to introduce key methods and tools for transforming problems into SDPs, and for manipulating and analysing those SDPs. These methods and tools are those which we believe to be very useful for a reader who wants semidefinite programming to be a useful tool in

---

<sup>1</sup> Throughout this book we will use the acronym SDP to denote both *semidefinite programming* and *semidefinite program*.

their research or work. In this respect, we encourage the reader to go through all chapters, even if the particular topic of the chapter is not so relevant for them; the way the topic is studied should hopefully teach them something new and interesting about semidefinite programming beyond the topic itself. In any case, we list the most important messages of each chapter in a section called *Concluding Remarks*.

The list of problems we cover are as follows:

- Chapter 3 addresses one of most basic problems in quantum physics, how to determine the properties of quantum states produced by an uncharacterised source. There are numerous variants of this problem, the most well-known being quantum state tomography, that is, estimating exactly which state the source is emitting. In this chapter we will review this and other variants of state estimation, including the so-called quantum marginal problem. This will allow us to study various aspects of SDPs, including how to obtain certificates of infeasibility and the prevalent notion of a ‘witness’.
- In chapter 4, we shift focus to quantum measurements. We will first discuss the problem of estimating which measurement a given measuring device is performing. We then study quantum state discrimination, the problem of determining—by performing a measurement—which state, out of a set of possibilities, a given source is producing. We show how to gain new insight into this problem by using the key concept of SDP duality, and how the tool of complementary slackness can be used to derive optimality conditions.
- We then move on to the problem of characterising quantum entanglement in chapter 5. Entanglement is nowadays seen as the main resource behind many quantum information tasks, such as quantum teleportation, computation and cryptography. In this chapter we will see how SDPs can be used to detect and quantify entanglement. We will also see how we can use a sequence—or hierarchy—of semidefinite programs to obtain approximations to the set of separable quantum states, and therefore bounds on many quantities of interest.
- In chapter 6 we will study one of the most basic and interesting properties of quantum mechanics: measurement incompatibility. We will see how this problem can be solved by semidefinite programming, and use duality to uncover an unexpected link to quantum nonlocality.
- Finally, in chapter 7 we will study quantum channels. We will see how the so-called Choi–Jamiołkowski isomorphism—which links quantum channels with quantum states—allows for semidefinite programming techniques to be applied to quantum channels. We will then see how we can estimate an uncharacterised channel, calculate the diamond norm (which characterises the operational distinguishability between channels) and finally how to use duality to uncover a link between a channel optimisation problem and quantum entropies.

At the end of each chapter we also suggest a small amount of additional material on each topic (in the section *Further reading*). It is important to note that the list of references is by no means exhaustive. Our aim is simply to provide the curious reader

with further resources—in the form of relevant textbooks or review articles—to complement the present text. In this connection, let us stress that there are several texts on semidefinite programming that can be used to complement this book in general. In particular, the book *Convex Optimization* by S Boyd and L Vandenberghe is a must-have reference on convex optimisation, which includes and goes beyond the theory of SDPs, and provides the reader with a comprehensive amount of information on the subject (and is freely available!). More related to quantum information are the textbook *The Theory of Quantum Information* and lecture notes *Theory of Quantum Information* by J Watrous and the lecture notes *Semidefinite Programming & Quantum Information* by J Sikora and A Varvitsiotis, all of which are freely available online.

Finally, this book is very much just an introduction to the topic of semidefinite programming. There are many more advanced topics that we chose not to cover here. Our goal was to provide a solid foundation to the key aspects of the theory, and to demonstrate their widespread applicability in quantum information science. We hope that using this book as a foundation, those readers who choose to do so, will be well placed to go on and master more advanced aspects of semidefinite programming—and more generally convex optimisation—and put them to good use in whichever direction they see fit.

---

## Part II

Semidefinite programming in quantum  
information science



# Semidefinite Programming in Quantum Information Science

**Paul Skrzypczyk and Daniel Cavalcanti**

---

## Chapter 3

### Quantum states

In this chapter we begin the second—and main—part of this book, where we explore the use of semidefinite programming in the context of quantum information science. As will be seen, semidefinite programming proves to be a versatile and powerful tool, which finds widespread and varied applications.

One of the first reasons why SDPs are so useful in quantum information is because—mathematically—quantum states are positive semidefinite operators,  $\rho \geq 0$ , which are normalised,  $\text{tr}(\rho) = 1$ . Being a linear operator inequality and an equality constraint respectively, these conditions can be used as constraints inside SDPs, so that many problems involving optimisation over quantum states can be cast as SDPs. In this chapter we will describe some of these problems. We will discuss problems related to *quantum state estimation*, which refers to the question of estimating the state that a source produces given the outcome statistics of a set of measurements. In the case this set of measurements is tomographically complete, this is equivalent to quantum state tomography—characterising the state emerging from a source. Sometimes, however, the information obtained experimentally is not enough to single out a unique quantum state. With the help of SDPs we can nevertheless characterise the set of states compatible with a given set of experimental observations, and estimate additional (unmeasured) properties of quantum states.

Altogether, these topics will allow us to see how problems involving quantum states can be cast as SDPs, and to use various aspects of the theory of SDPs presented in the previous chapters, in order to gain important insights about these problems.

We will end this chapter with a brief section on the *quantum marginal problem*, which can be viewed as a generalisation of quantum state estimation. In this problem, we consider *multipartite* systems, and are given complete information only about some of their *subsystems*. The goal is then to determine the global state, or properties of it. As will be seen, the tools of semidefinite programming can also be used to solve this problem, and leads to a simple way to see when certain sets of marginals are inconsistent with each other.

### 3.1 Quantum state estimation

Suppose an experimentalist comes to you and says

*I have a source of spin-1/2 particles (i.e. qubits) in my laboratory, that I have measured along two different spin directions  $\hat{x}$  and  $\hat{y}$ , obtaining the following expectation values:  $\langle \sigma_x \rangle = 0.9$  and  $\langle \sigma_y \rangle = 0.5$ ,*

where  $\sigma_x$ ,  $\sigma_y$  and  $\sigma_z$  are the three Pauli operators. Is there any way to know if they are telling the truth or not? More precisely, is it possible to determine whether what they claim to have observed is consistent with the predictions of quantum mechanics? The simple situation above can indeed be checked through basic algebraic means, using the properties of the measurements used. But in more complicated and sophisticated situations, involving, e.g. many measurements with no symmetry relations between them, or high-dimensional quantum system, the task becomes more intricate.

However, this problem can in fact be cast as a simple feasibility SDP. Namely, suppose that we are given the measurement results for a set of  $N$  observables  $M_1, \dots, M_N$ . Let us assume that we are only told the *average* values of each measurement,  $\langle M_1 \rangle = m_1, \dots, \langle M_N \rangle = m_N$ . Our goal is to check if these reported values are compatible with some quantum state  $\rho$ . This amounts to solving the following feasibility SDP:

$$\text{find } \rho \tag{3.1a}$$

$$\text{subject to } \text{tr}(M_x \rho) = m_x \quad x = 1, \dots, N, \tag{3.1b}$$

$$\text{tr}(\rho) = 1, \tag{3.1c}$$

$$\rho \geq 0. \tag{3.1d}$$

There are three possibilities that can arise.

1. **Unique solution.** The set of observables  $\{M\}$  we consider might have the property of being *tomographically complete*. This means that knowing the results for every measurement in the set is sufficient to uniquely determine the state. Mathematically, the set must have a sufficient number of linearly independent measurements in order to determine all of the matrix elements of the density operator  $\rho$ . In this case, the feasible set of the SDP is a unique density operator  $\mathcal{F} = \rho^*$ .
2. **No solution.** The other extreme case is when there is *no solution*, i.e. there is no quantum state  $\rho$  which is able to produce the desired list of expectation values (and the experimentalist was lying or mistaken). In this case, the SDP is *infeasible*, and we see that the feasible set must be empty,  $\mathcal{F} = \emptyset$ . We will study this in detail in section 3.1.5, where it is shown that the dual SDP can be used to provide us with a certificate, which will convince us that there is no quantum state producing the desired set of expectation values.

3. **Multiple solutions.** The situation in between the above two cases is that there are infinitely many states  $\rho$  which produce the given set of expectation values. This means that the set of measurements is not tomographically complete, such that they do not uniquely determine all of the matrix elements of the density operator. On the other hand, the expectation values are consistent with each other. In terms of the SDP, here the feasible set  $\mathcal{F}$  will be non-empty, and contain more than a single state.

### 3.1.1 Trace distance estimation

The above shows that quantum state estimation can be cast as an SDP. We can however use semidefinite programming to dig much deeper into the problem of state estimation. As a first example, imagine that not only do we have the set of measurement results, but also a *target state*, that we believe was prepared, and which was measured to produce the observed statistics. If the statistics are incompatible with this target state we might be interested in understanding *how close* the prepared state was to the target state.

In this section we will see that this question can be answered using semidefinite programming. In particular, we will show that it is possible to find the *best-case* trace distance between any state consistent with the measurement results and some target state.

The key ingredient is to use the primal SDP formulation for the trace norm, as given in (2.8), which we will see can be harnessed here for our needs.

Recall that for a pair of quantum states the trace distance is given by

$$T(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1. \quad (3.2)$$

This is a non-linear function of  $\rho$  and  $\sigma$ , and so cannot be used directly as either the objective function or as a constraint inside an SDP. However, as we saw in example 2.3 in the previous chapter, it can nevertheless be possible to recast problems which appear non-linear as SDPs. We will see here that trace distance estimation is indeed such a problem where the non-linearity is not a road block. The first thing to note is that although non-linear, the trace distance is nevertheless a convex function of either state, such that

$$T(q\rho_0 + (1 - q)\rho_1, \sigma) \leq qT(\rho_0, \sigma) + (1 - q)T(\rho_1, \sigma), \quad (3.3)$$

and similarly for the second state.

There are two possibilities that are of potential interest—the *best case* and the *worst case*. In the former, we would want to find the *closest* state to our target state consistent with the measurement results. On the other hand, in the latter case, we would seek to find the state which is furthest away from our target state and still consistent with the results.

The fact that the trace distance is convex means that we will not be able to analyse the *worst case*, but only the best case. Why is this? This is in fact an important lesson about convex optimisation—more general than just linear programs (LPs) and SDPs. As the following sketch illustrates, *convex* objective functions are naturally

associated with *minimisation* problems and *concave* objective functions are naturally associated with *maximisation* problems: maximising a convex function we are led to the extremes of the function—to the boundary of the domain. This is a fundamentally different type of optimisation problem compared with finding the optima, which naturally occur at *stationary points*.

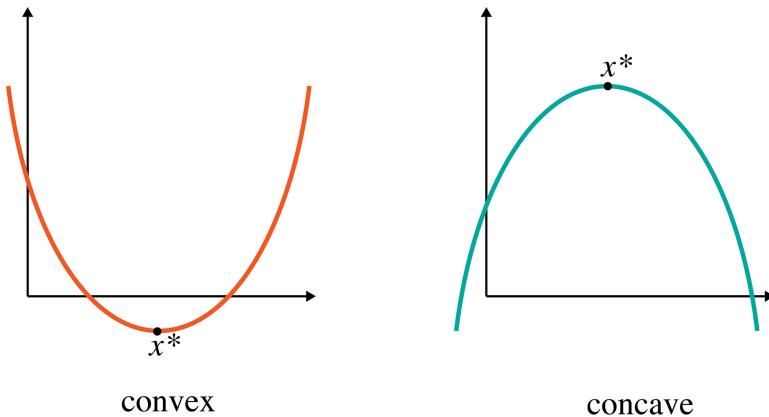
Since the trace distance is convex, we can consider problems involving its minimisation, which here would correspond to finding the *minimal distance* or *closest state* to the target state. In particular, the problem we can attempt to solve is

$$\text{minimise} \quad \frac{1}{2} \|\rho - \sigma\|_1 \quad (3.4a)$$

$$\text{subject to} \quad \text{tr}(M_x \rho) = m_x \quad x = 1, \dots, N, \quad (3.4b)$$

$$\text{tr}(\rho) = 1, \quad (3.4c)$$

$$\rho \geq 0. \quad (3.4d)$$



This is still not an SDP, but it can be turned into one by making use of example 2.3, in particular (2.8), which gave an SDP for the trace norm  $\|A\|_1$  of an arbitrary Hermitian operator  $A$ . Here there are two additional complications: (i) whereas previously  $A$  was the *data* of the problem, here  $A = \rho - \sigma$  is instead a *variable*; (ii) as stated above, we now want to *minimise* the trace norm rather than just calculate it. Luckily both of these complications are harmless. First, in (2.8) the variable  $X$  is never multiplied by the data  $A$ . Thus, although here  $A = \rho - \sigma$  is now a variable, it doesn't actually stop the problem from being linear, and therefore from being an SDP.

Second, since the SDP (2.8) for the trace norm is a minimisation, and we want to consider here the *best case*—itself corresponding to *minimisation*—we end up with a double minimisation. However, double minimisations are still convex optimisation problems, and in this case our problem *remains an SDP*. Altogether, we arrive at the

following SDP for finding the closest state in trace distance to a target state, given the measurement results:

$$\text{minimise} \quad \frac{1}{2}\text{tr}(\textcolor{brown}{X}) \quad (3.5\text{a})$$

$$\text{subject to} \quad -\textcolor{brown}{X} \leq \textcolor{brown}{\rho} - \textcolor{blue}{\sigma} \leq \textcolor{brown}{X}, \quad (3.5\text{b})$$

$$\text{tr}(\textcolor{teal}{M}_x \textcolor{brown}{\rho}) = \textcolor{teal}{m}_x, \quad x = 1, \dots, N \quad (3.5\text{c})$$

$$\text{tr}(\textcolor{brown}{\rho}) = 1, \quad (3.5\text{d})$$

$$\textcolor{brown}{\rho} \geq 0. \quad (3.5\text{e})$$

Incidentally, we can now understand mathematically why it is not possible to analyse the worst case, i.e. to find the state which is as far as possible from the target state. In such a case, we would end up with almost the same problem as (3.4), except the objective would now be to maximise, rather than minimise. However, we would then not be able to end up at a form like (3.5), since there it was possible to combine the two minimisations—one over  $\rho$  and one over  $X$ —into a single minimisation, and obtain an SDP. To evaluate the worst case, we would need to maximise over  $\rho$  and minimise over  $X$ , and these *cannot be combined* into a single optimisation. This reflects the fact that to find the worst case, as already realised, would require maximising a convex function, which is a fundamentally different type of problem.

### 3.1.2 Fidelity estimation

We now turn our attention to a second notion of closeness between states—namely the fidelity. We will start by specialising to the problem of determining how close  $\rho$  is to a *pure* quantum state  $\sigma = |\psi\rangle\langle\psi|$ . As will be seen, this is more straightforward than the general problem of estimating the fidelity to a *mixed* state. In particular, the fidelity between a state  $\rho$  (which can be either mixed or pure) and a pure state  $\sigma = |\psi\rangle\langle\psi|$  is

$$F(\rho, \sigma) = \langle\psi|\rho|\psi\rangle = \text{tr}(|\psi\rangle\langle\psi|\rho), \quad (3.6)$$

which, notably, is a *linear* function of  $\rho$ . We can thus use this as the objective function directly, and arrive at the following SDP to find the closest state in fidelity to a target state, i.e. the state with *maximum fidelity* with the target state  $\sigma = |\psi\rangle\langle\psi|$ ,

$$\text{maximise} \quad \text{tr}(|\psi\rangle\langle\psi|\rho) \quad (3.7\text{a})$$

$$\text{subject to} \quad \text{tr}(\textcolor{teal}{M}_x \rho) = \textcolor{teal}{m}_x \quad x = 1, \dots, N, \quad (3.7\text{b})$$

$$\text{tr}(\rho) = 1, \quad (3.7\text{c})$$

$$\rho \geq 0. \quad (3.7\text{d})$$

This SDP again allows us to understand the *best case*, i.e. the largest fidelity among all possible states that are compatible with the observed data.

Interestingly, since the fidelity is linear, we can now consider the associated *minimisation* problem, i.e. to replace the maximisation in (3.7) by a minimisation. In this case, we then find the *worst-case* fidelity, i.e. the smallest fidelity among all possible states consistent with the measurement results.

This is somewhat surprising, since we saw for the trace distance that it isn't possible to obtain the worst-case state. The key difference here is that the fidelity to a pure state is linear, meaning it is both *convex and concave*, and so we can in fact also solve the worst-case problem too. Unfortunately, as will be seen below, this is a special property of the fidelity with pure states. In the more general case, of fidelity with a mixed target state, it is again only possible to solve the best-case scenario.

Moving on to the more general problem of estimating the fidelity between two mixed states, the general expression for the fidelity is given by

$$F(\rho, \sigma) = \left\| \sqrt{\rho} \sqrt{\sigma} \right\|_1^2, \quad (3.8a)$$

$$= \left[ \text{tr}(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}) \right]^2, \quad (3.8b)$$

which is now a non-linear function of both  $\rho$  and  $\sigma$ . This means that, just as with the trace distance, we can no longer directly use this as the objective function in an SDP. Although non-linear, the fidelity is nevertheless a *concave* function (in either state), meaning that

$$F(q\rho_0 + (1 - q)\rho_1, \sigma) \geq qF(\rho_0, \sigma) + (1 - q)F(\rho_1, \sigma), \quad (3.9)$$

for  $q \in [0, 1]$ , and similarly for  $\sigma$ . This says that the fidelity between the average state  $\rho' = q\rho_0 + (1 - q)\rho_1$  and  $\sigma$  is never smaller than the average of the fidelities between  $\rho_0$  and  $\sigma$  and  $\rho_1$  and  $\sigma$ .

The fact that the fidelity is concave means—once again—that it will only be possible to estimate the *best-case* fidelity, since we will be able to consider *maximising* the fidelity (and now a larger fidelity means a closer state), given the constraints arising from the measurements result.

The difficulty that must still be overcome is to understand how we can evaluate the fidelity objective function using semidefinite programming. We will return to this topic in more detail in the ‘Advanced topics’ section 3.5.1, but just as with the trace distance, even though the fidelity is a non-linear function, it can nevertheless be expressed as an SDP by introducing auxiliary variables. As shown in section 3.5.1, the square-root-fidelity is in fact given by the following SDP:

$$\sqrt{F(\rho, \sigma)} = \text{maximise } \text{tr}(Y) \quad (3.10a)$$

$$\text{subject to } \begin{pmatrix} \rho & Y + iZ \\ Y - iZ & \sigma \end{pmatrix} \geq 0. \quad (3.10b)$$

We have written the constraint (3.10b) in a relatively intuitive way, arranging the variables  $\mathbf{Y}$  and  $\mathbf{Z}$  into a *block matrix*, along with the data of the problem—the quantum states  $\rho$  and  $\sigma$ . It is important to appreciate that this inequality constraint is equivalent to the standard form as in (2.1c), namely of the form  $\Gamma(\mathbf{X}) \leq C$ . In particular, since we have a pair of variables  $\mathbf{Y}$  and  $\mathbf{Z}$ , we have a map  $\Gamma(\mathbf{Y}, \mathbf{Z})$ , which can be written

$$\Gamma(\mathbf{Y}, \mathbf{Z}) = |\mathbf{0}\rangle\langle\mathbf{0}| \otimes \rho + |\mathbf{0}\rangle\langle\mathbf{1}| \otimes (\mathbf{Y} + i\mathbf{Z}) + |\mathbf{1}\rangle\langle\mathbf{0}| \otimes (\mathbf{Y} - i\mathbf{Z}) + |\mathbf{1}\rangle\langle\mathbf{1}| \otimes \sigma \quad (3.11)$$

with a similar technique applicable for any block matrix. As can be seen, the block matrix form of (3.10b) is much easier to read than the form of (3.11), and hence we will use the block form whenever appropriate to do so.

Returning to the problem of estimating the largest fidelity with a target state, we can now directly use (3.10) in order to recast the problem as an SDP. In particular, the following SDP is arrived at, which evaluates the best-case (square-root) fidelity between any state  $\rho$  consistent with the data, and a target state  $\sigma$ :

$$\text{maximise} \quad \text{tr}(\mathbf{Y}) \quad (3.12a)$$

$$\text{subject to} \quad \begin{pmatrix} \rho & \mathbf{Y} + i\mathbf{Z} \\ \mathbf{Y} - i\mathbf{Z} & \sigma \end{pmatrix} \geq 0, \quad (3.12b)$$

$$\text{tr}(\mathbf{M}_x \rho) = m_x \quad x = 1, \dots, N, \quad (3.12c)$$

$$\text{tr}(\rho) = 1, \quad (3.12d)$$

$$\rho \geq 0. \quad (3.12e)$$

Note that, compared with the SDP formulation of  $\sqrt{F(\rho, \sigma)}$ , we have relaxed  $\rho$  from being *input data* to being a *variable*, constrained by the measurement results. Crucially, as can be seen, this problem remains *linear*, and subsequently remains an SDP. We can also note that, just as for the trace distance, the above works since the SDP formulation of the fidelity was a *maximisation* problem. By relaxing  $\rho$ , the best-case state given the constraints, is now naturally found.

In principle, distances other than the trace distance and fidelity can also be considered in state estimation. As the above two examples have hopefully demonstrated, these distances need not be linear functions, but they must be expressible themselves as SDPs.

### 3.1.3 Finite statistics

We now turn our attention to a different aspect of quantum state estimation, that of *finite statistics*. In practice, due to the fact that every experiment can only handle a finite number of measurement rounds, it is rather unreasonable to assume that the expectation values  $m_1, \dots, m_N$  are known exactly. In reality, these will have been estimated themselves, and will only be known up to some level of uncertainty. Let us therefore assume that the result of each measurement is only known to lie in some

interval  $[m_x - \Delta_x, m_x + \Delta_x]$ . The problem of interest now is the feasibility problem of determining whether there is a quantum state  $\rho$  which is consistent with all of these uncertain expectation values,

$$\text{find } \rho \quad (3.13a)$$

$$\text{subject to } m_x - \Delta_x \leq \text{tr}(M_x \rho) \leq m_x + \Delta_x \quad x = 1, \dots, N, \quad (3.13b)$$

$$\text{tr}(\rho) = 1, \quad (3.13c)$$

$$\rho \geq 0, \quad (3.13d)$$

where to aid presentation we have displayed *both* inequality constraints related to the measurement intervals in a single line for each expectation value. Each equality constraint from the original problem (3.1) is thus replaced by a pair of inequality constraints. As will be seen later, this will have an effect on the *dual SDP*—which will have twice as many dual variables compared to the dual of the original problem.

From the perspective of the structure of the SDP, since there are no equality constraints relating  $\rho$  with the observed data in this problem, even if the set of measurements  $\{M_x\}_x$  is tomographically complete, in general we would never expect to find a *unique* solution, unlike before. This is rather natural, as we would expect to have some residual uncertainty about the state, given the uncertainty in the measurement results, whenever they are consistent.

### 3.1.4 Relaxing the feasibility problem

In another direction, we return now to our original feasibility problem of quantum state estimation, as given in (3.1), and look at how it can be relaxed to an optimisation problem. There are a few of reasons for doing this. First, it will allow us to understand *quantitatively* how inconsistent a set of measurement results are, whenever there is no state that can lead to them. Second, from a numerical perspective, it is useful to be able to transform feasibility problems into optimisation problems, which are generally much more stable to solve. Finally, having an optimisation form will allow us to use duality, which we will show to be useful in later sections.

There are multiple ways in which the feasibility problem (3.1) can be relaxed to an optimisation problem, each with their relative merits. Here we will adapt the approach from the previous section on finite statistics, in order to obtain a relaxation of the problem, which is *always feasible*.

The key idea is to relax the equality constraints (3.1b)—to not demand that the observed expectation values are reproduced exactly, but allow them to be reproduced *approximately*, in a very similar fashion to the above section. Whereas in the above the relaxation was coming from the uncertainty due to finite statistics, here the logic is different. Here we seek to find a set of measurement results which *best*

approximates the target results. If they can be reproduced exactly, then the original problem was feasible, and hence we obtain a quantum state  $\rho$  that can reproduce the statistics. If on the other hand the problem is infeasible, it will be necessary to perturb the results in order for them to be producible by some quantum state. The crucial observation is that *a sufficiently big perturbation of the results will always be producible by some quantum state*. This means that this relaxation will lead to an SDP which will be *feasible by construction*. Finally, by minimising the size of the perturbation, the best approximation is found.

It is interesting to note that this approach can be seen as complementary to that taken in sections 3.1.1 and 3.1.2 on trace distance and fidelity estimation. In particular, in those sections, in essence we sought to find the state which best approximated a target state. Here, on the other hand, we seek to find the set of measurement results which best approximates the target measurement results.

A simple way to achieve the above relaxation is to place a *uniform bound* on how much any single result can differ from the desired result. That is, we introduce a new variable  $\delta$ , and replace the equality constraints (3.1b) with pairs of inequality constraints

$$m_x - \delta \leq \text{tr}(M_x \rho) \leq m_x + \delta \quad x = 1, \dots, N. \quad (3.14)$$

This enforces that for all measurements,  $|\text{tr}(M_x \rho) - m_x| \leq \delta$ . The reason for writing this in the form (3.14) is that in this form the constraint is manifestly linear in all of the variables. It is also worth noting that this is very similar to (3.13b), the difference being that previously the uncertainties  $\Delta_x$  depended upon the measurement, and were input data to the problem, whereas here we simplify and consider only a single  $\delta$ , which is now constant and a variable of the problem. Putting everything together, we arrive at the following relaxed SDP for quantum state estimation:

$$\text{minimise} \quad \delta \quad (3.15a)$$

$$\text{subject to} \quad m_x - \delta \leq \text{tr}(M_x \rho) \leq m_x + \delta \quad x = 1, \dots, N, \quad (3.15b)$$

$$\text{tr}(\rho) = 1, \quad (3.15c)$$

$$\rho \geq 0. \quad (3.15d)$$

Any solution with  $\delta = 0$  satisfies all of the constraints of the original problem (3.1). On the other hand, when  $\delta^* > 0$ , this signifies that the original problem (3.1) is infeasible, and there is no quantum state able to reproduce the data.

It is important to realise that  $\delta^*$  provides us with quantitative information regarding how close the problem is to being feasible: if  $\delta^*$  is small this means that there is a quantum state that is able to reproduce closely the measurement results; on the other hand, if  $\delta^*$  is large, at least one of the measurement results needs to be significantly different from that observed, in order to be producible by some quantum state.

### Exercises

- 3.1 By defining vectors  $\vec{m}$  with components  $m_x$  and  $\vec{m}'$  with components  $m'_x = \text{tr}(\mathcal{M}_x \rho)$ , show that the SDP (3.15) can also be written as

$$\begin{aligned} & \text{minimise} && \|\vec{m}' - \vec{m}\|_\infty \\ & \text{subject to} && m'_x = \text{tr}(\mathcal{M}_x \rho) \quad x = 1, \dots, N, \\ & && \text{tr}(\rho) = 1, \\ & && \rho \geq 0. \end{aligned}$$

*This shows that this relaxation can be understood as minimising the  $\ell_\infty$  distance between the target data  $\vec{m}$ , and any set of data that can be produced in quantum mechanics.*

- 3.2 Write down the SDP relaxation of (3.1) which minimises instead the  $\ell_1$  distance  $\frac{1}{2}\|\vec{m} - \vec{m}'\|_1$ , between the target data  $\vec{m}$ , and data that can be produced in quantum mechanics  $\vec{m}'$ .

### 3.1.5 Certificate of infeasibility

We now consider the situation where we are given some experimental data which is inconsistent, such that there is no quantum state that could possibly lead to this data. An interesting question is: can we certify that this is the case without having to numerically solve the SDP? Is there an *analytic* certificate that can be used to prove unequivocally that the SDP is infeasible? In this section it will be seen that duality allows us to provide such a simple *certificate*, which will convince us whenever a set of measurement results is inconsistent. This idea is rather general, and can be widely applied to guarantee that an given SDP is infeasible.

Our starting point will be the relaxed problem (3.15). Recall that we attempt to minimise  $\delta$ , and if we are able to find a solution  $\delta = 0$ , then the associated state  $\rho$  will be consistent with the measurement results. On the other hand, if  $\delta^* > 0$ , then the results are inconsistent. In what follows we will show how duality can be used to guarantee that  $\delta^* > 0$  without having to solve the SDP. Recall that for a minimisation problem, the values that the dual objective function can take always lower bound the optimal value of the primal problem (weak duality). Therefore, if we can find a set of dual variables such that the value of the dual objective function is strictly positive, then *with certainty* the primal problem has  $\delta^* > 0$ . It is precisely a collection of dual variables that lead to a positive value of the dual objective function that will constitute our certificate. Let us now put this into practice.

By introducing scalar dual variables  $u_x$  and  $v_x$  associated to the first and second inequality constraint respectively in (3.15b), a scalar  $z$  associated to (3.15c) and an operator  $W$  associated to (3.15d), the associated Lagrangian of the problem is

$$\mathcal{L} = \delta - \sum_{x=1}^N u_x [\text{tr}(\mathcal{M}_x \rho) - m_x + \delta] - \sum_{x=1}^N v_x [m_x + \delta - \text{tr}(\mathcal{M}_x \rho)] + z[1 - \text{tr}(\rho)] - \text{tr}(W\rho), \quad (3.16a)$$

$$= \delta \left[ 1 - \sum_{x=1}^N (u_x + v_x) \right] + \text{tr} \left[ \rho \left( \sum_{x=1}^N (v_x - u_x) \mathcal{M}_x - z \mathbb{I} - W \right) \right] + z + \sum_{x=1}^N (u_x - v_x) m_x. \quad (3.16b)$$

Note that since the primal problem is a minimisation problem, the Lagrangian is constructed to be smaller than the value of the primal objective function for all primal feasible variables, and hence we take  $u_x \geq 0$ ,  $v_x \geq 0$  and  $W \geq 0$ . Recall that this is the reason for the additional minus signs in the Lagrangian in the second, third and last term, which arise whenever we construct the Lagrangian for a minimisation problem, as shown in exercise 2.11. We can additionally make the Lagrangian independent of the primal variables by ensuring the first and second brackets vanish in (3.16b). Maximising, to obtain the best lower bound, and solving for  $W$ , which is seen to play the role of a slack variable, we arrive at the dual formulation

$$\text{maximise} \quad z + \sum_{x=1}^N (u_x - v_x) m_x \quad (3.17a)$$

$$\text{subject to} \quad zI + \sum_{x=1}^N (u_x - v_x) M_x \leq 0, \quad (3.17b)$$

$$\sum_{x=1}^N (u_x + v_x) = 1, \quad (3.17c)$$

$$u_x \geq 0 \quad v_x \geq 0 \quad x = 1, \dots, N. \quad (3.17d)$$

Let us now analyse this dual a little. The first thing to notice is that the constraints (3.17c) and (3.17d), together with the fact that everywhere else only the combination  $u_x - v_x$  appears, shows that the problem can be interpreted as one of optimising over a single dual variable  $\vec{t} = \vec{u} - \vec{v}$ , with components  $t_x = u_x - v_x$ , such that  $\|\vec{t}\|_1 \leq 1$ . This can be seen from the definition of the  $\ell_1$  unit ball from (1.62). Thus, we can express (3.17) in a simpler form:

$$\text{maximise} \quad z + \vec{t} \cdot \vec{m} \quad (3.18a)$$

$$\text{subject to} \quad zI + \vec{t} \cdot \vec{M} \leq 0, \quad (3.18b)$$

$$\|\vec{t}\|_1 \leq 1, \quad (3.18c)$$

where we have introduced an *operator vector*  $\vec{M} = (M_1, \dots, M_N)$ , the components of which are the observables, and, as above,  $\vec{m} = (m_1, \dots, m_N)$  is the vector whose components are the measurement results.

How does this serve as a certificate for the fact that the measurement results  $\vec{m}$  were inconsistent? Let us assume that we have found a set of dual feasible points—i.e. a set of dual variables  $(z, \vec{t})$  satisfying the constraints—such that  $\beta = z + \vec{t} \cdot \vec{m} > 0$ . Now, consider the constraint (3.18b), and multiply both sides by an arbitrary quantum state  $\rho$  and take the trace. We see that

$$\text{tr}[\rho(zI + \vec{t} \cdot \vec{M})] = z + \sum_{x=1}^N t_x (\rho M_x) \leq 0. \quad (3.19)$$

The first equality follows from the linearity of the trace, while the second follows from the fact that for two operators  $A \geq 0$  and  $B \leq 0$ , we have  $\text{tr}(AB) \leq 0$ . What this shows is that the operator inequality (3.18b) guarantees that any set of measurement results  $\vec{m}' = (\text{tr}(\rho \vec{M}_1), \dots, \text{tr}(\rho \vec{M}_N))$  that can arise by performing measurements on a quantum state, will never lead to a positive value of  $\beta$ . This shows that the claim that the purported results  $\vec{m}$  were observed, must have been false. The dual problem is thus seen to look for a carefully chosen set of dual variables  $(z, \vec{t})$  such that on the one hand, the purported results lead to a positive value of the dual objective function, while simultaneously demanding that all valid measurement results lead to a negative value. In the next section we will explore the geometry of this, but as a preview, what we have just observed can be thought of as a *separation* between what is allowed and what is not allowed, and is a common geometrical feature of certificates of this type.

Why is this better than solving the primal SDP in (3.1)? There are a number of advantages. First, given the dual variables, no optimisation is required in order to check whether the following two conditions hold: (i)  $\beta = z + \vec{t} \cdot \vec{m} > 0$ , and (ii) all of the eigenvalues of  $W = z\mathbb{I} + \vec{t} \cdot \vec{M}$  are negative. Second, this certificate can in principle even be checked analytically, that is, we can analytically evaluate  $\beta$  and find the eigenvalues of  $W$ , and thus verify analytically that all of the constraints of the dual are satisfied. This is in contrast to only having a numerical solution for the primal problem. Finally, although this certificate is designed for a given set of inconsistent data  $\vec{m}$ , it can be used more universally, to check the inconsistency of *any* data. In particular, although it may fail to identify inconsistent data, if any set of data leads to a strictly positive value of  $\beta$ , then it is guaranteed to be inconsistent. We exemplify this in the following example:

### Example 3.1 Equatorial plane of the Bloch sphere

In this example, we will show how the above dual SDP (3.18) can in fact be used as a method to derive the equator of the Bloch sphere. That is, any qubit, written in the form  $\rho = (\mathbb{I} + \vec{r} \cdot \vec{\sigma})/2$ , with  $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$  the vector of Pauli operators and  $\vec{r}$  the Bloch vector with components  $r_i = \text{tr}(\sigma_i \rho)$ , will be a valid density operator only if  $r_x^2 + r_y^2 \leq 1$ .

In order to obtain this result, assume that two Pauli measurements are performed,  $\vec{M} = (\sigma_x, \sigma_y)$ . We will use (3.18) to find the allowed measurement results  $\vec{m} = (m_x, m_y)$  that can arise—and in so doing re-derive the equatorial plane of the Bloch sphere.

From (3.18b), we are seeking dual variables that satisfy

$$z\mathbb{I} + t_x \sigma_x + t_z \sigma_z \leq 0 \quad (3.20)$$

and from (3.18c), we furthermore must have  $\|\vec{t}\|_1 = |t_x| + |t_z| \leq 1$ . Since any operator of the form  $n_x \sigma_x + n_y \sigma_y$  has eigenvalues  $\pm 1$  whenever  $\|\vec{n}\|_2 = \sqrt{n_x^2 + n_y^2} = 1$ , we see that the eigenvalues of the operator  $z\mathbb{I} + t_x \sigma_x + t_y \sigma_y$  are

$$\lambda_{\pm} = z \pm \|\vec{t}\|_2, \quad (3.21)$$

and so we will satisfy (3.20) whenever

$$\textcolor{red}{z} + \|\vec{t}\|_2 \leq 0. \quad (3.22)$$

We can therefore take  $\textcolor{red}{z} = -\|\vec{t}\|_2$ , so that the inequality is saturated. With this choice of  $\textcolor{red}{z}$ , the dual objective function is

$$-\|\vec{t}\|_2 + \vec{t} \cdot \vec{m}. \quad (3.23)$$

Now, any set of measurement outcomes  $\vec{m} = (m_x, m_y)$  for which this is strictly positive is inconsistent, since we have just arranged it such that this can never happen. That is,  $\vec{m}$  is inconsistent if

$$\vec{t} \cdot \vec{m} > \|\vec{t}\|_2. \quad (3.24)$$

Up to this point, we still haven't specified  $\vec{t}$ , other than the requirement that  $\|\vec{t}\|_1 \leq 1$ . Let us therefore choose

$$\vec{t} = \frac{\vec{m}}{\|\vec{m}\|_1}. \quad (3.25)$$

This implies that  $\|\vec{t}\|_2 = \|\vec{m}\|_2 / \|\vec{m}\|_1$ , and so the data is inconsistent whenever

$$\|\vec{m}\|_2^2 > \|\vec{m}\|_1, \quad (3.26)$$

i.e.  $\|\vec{m}\|_2 > 1$ . In other words, consistent measurement outcomes must satisfy  $\|\vec{m}\|_2 \leq 1$ . Written out in full, this equates to  $m_x^2 + m_y^2 \leq 1$ . Since  $\vec{m}$  is nothing but the components of the Bloch vector of a qubit in the equatorial plane, this re derives the equatorial plane of the Bloch sphere.

Of course this result is well-known and can be obtained more directly, by finding the eigenvalues of a qubit density operator—we did not need to resort to the duality theory of SDPs to derive this result. However, the utility of going through this example is that in more complicated situations, involving for example non-Pauli measurements, or higher dimensions, this approach can still be applied, and provides a general method that can be used to understand the limitations of the quantum state space, and the measurement statistics it leads to.

As an exercise below, this same procedure is carried out with all three Pauli measurements, from which the entire Bloch sphere of a qubit can similarly be recovered.

### Exercises

- 3.3 Apply the same argument as in exercise 3.1, but for data  $\vec{m} = (m_x, m_y, m_z)$  arising from the three Pauli measurements  $\vec{M} = (\sigma_x, \sigma_y, \sigma_z)$ , to show that the data is inconsistent whenever  $\|\vec{m}\|_2 > 1$ . Explain why this re derives the Bloch sphere.

### 3.1.6 Geometrical interpretation

We finish our exploration of quantum state estimation by investigating how the above certificates of infeasibility can be understood geometrically. Understanding

SDPs and their duality geometrically can be very powerful, and provides insight and intuition for how and why duality works.

Our starting point is to think geometrically about the *space of quantum states* and *space of measurement data*. The space of all quantum states of a fixed, finite dimension  $d$  is the set

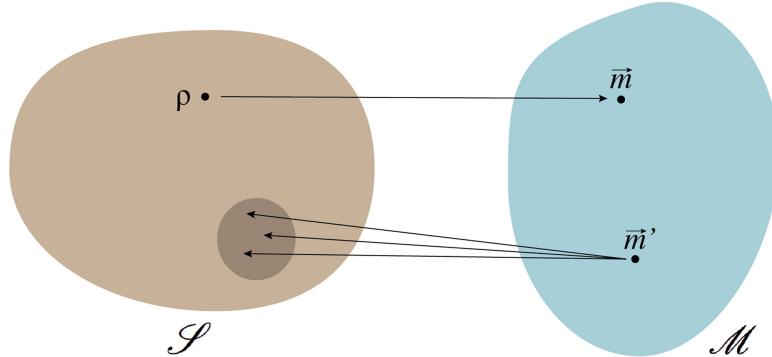
$$\mathcal{S} = \{\rho \mid \rho \geq 0, \text{tr}(\rho) = 1\}, \quad (3.27)$$

where  $\rho$  is an operator acting on  $\mathbb{C}^d$ . This is a convex set, which we can always visualise as a subset of  $\mathbb{R}^{d^2}$ . For a fixed set of measurements  $\tilde{\mathcal{M}}$ , the set of all quantum states  $\mathcal{S}$  gets mapped into a *space of measurement results*, which is the image of  $\mathcal{S}$  under the mapping

$$\rho \mapsto \vec{m} = (\text{tr}(\mathcal{M}_1\rho), \dots, \text{tr}(\mathcal{M}_N\rho)) \quad (3.28)$$

which can be represented as a subset of  $\mathbb{R}^N$ . We denote this image by  $\mathcal{M}$ . This mapping is illustrated in figure 3.1. Because this is a linear map, the convexity of the state space is preserved, and the space of all measurement results is also a convex set—see exercise 3.4.

We can understand many features of the state estimation problem from this geometrical perspective. First, note that the estimation problem is an *inverse problem*: we are given a point in the measurement space, and ask for the quantum state(s)  $\rho$  under the inverse mapping. When the set of measurements is not tomographically complete, then multiple states lead to the same set of measurement results. This shows that there is a *loss of information*. As such, there is not a unique solution to the inverse problem. In this case, the dimension of the measurement space will be smaller than the dimension of the state space. On the other hand, when

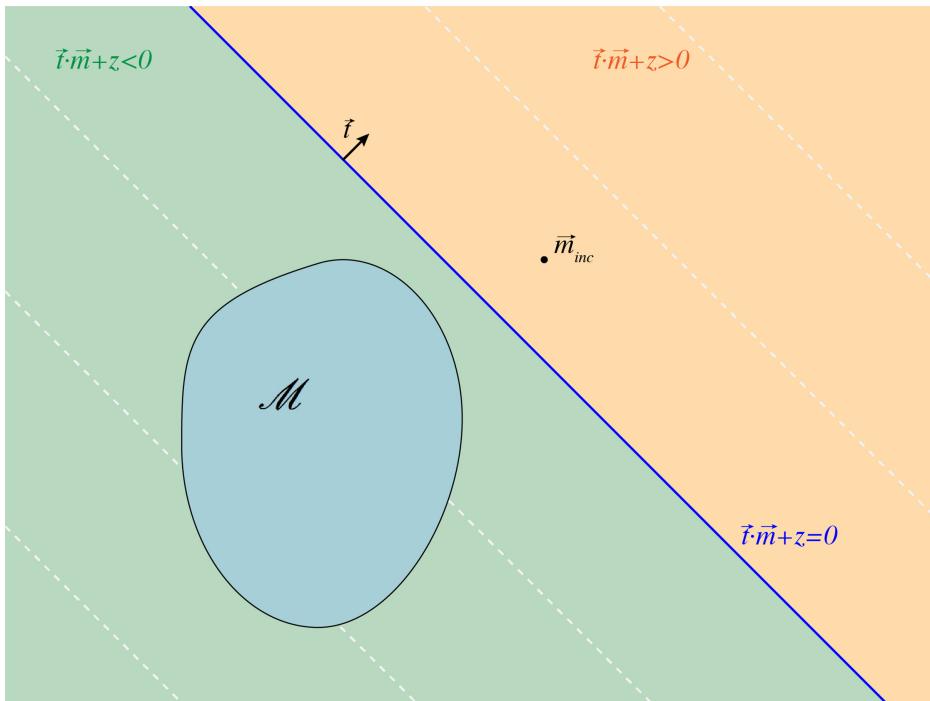


**Figure 3.1.** Mapping between state space and space of measurement results of a fixed set of measurements. An illustration of the mapping of the quantum state space  $\mathcal{S}$  into the set of measurement results  $\mathcal{M}$ , under the mapping  $\rho \mapsto \vec{m} = (\text{tr}(\mathcal{M}_1\rho), \dots, \text{tr}(\mathcal{M}_N\rho))$ . For illustrative purposes both spaces are depicted as being 2-D, although in general they are both high-dimensional bodies of different dimension. Each quantum state  $\rho$  is mapped to a single vector of measurement results  $\vec{m}$ . In general, the mapping can be many-to-one, with multiple quantum states being mapped to the same point in  $\mathcal{M}$ . This means that the inverse mapping, from a vector  $\vec{m}'$  leads to a subset of the state space  $\mathcal{S}$ , as depicted.

the measurements are tomographically complete, there is no loss of information and a one-to-one mapping between the two spaces. This implies that the dimension of the measurement space must be equal or greater to the dimension of the state space.

Most interestingly, we can gain insight into the certificate of infeasibility. Geometrically, if a fictitious set of measurement results  $\vec{m}_{\text{inc}}$  is inconsistent, this means it *lies outside of the image of  $\mathcal{S}$* . A remarkable fact from convex geometry now comes into play: *it is always possible to find a hyperplane which separates a point from a convex set*. This is somewhat obvious in one, two and three dimensions, and in fact it holds in all dimensions. The certificate of infeasibility is *precisely the specification of such a separating hyperplane*, as depicted in figure 3.2.

As we will see in many instances throughout this book, dual SDPs can often be interpreted as providing *certificates* or *witnesses* of certain properties, and these can be understood geometrically as specifying separating hyperplanes.



**Figure 3.2.** Geometric interpretation of certificate of infeasibility. An illustrative example in 2-D of how the certificate of infeasibility can be viewed as a *separating hyperplane* where  $z + \vec{t} \cdot \vec{m} = 0$ , which separates  $\mathcal{M}$ —the image of  $\mathcal{S}$  (blue set)—from the supposed set of measurement results  $\vec{m}_{\text{inc}}$ . The vector  $\vec{t}$  specifies a direction, and  $z$  specifies an offset, such that the image of  $\mathcal{S}$  lies in the (green) region where  $z + \vec{t} \cdot \vec{m} < 0$  and  $\vec{m}_{\text{inc}}$  lies in the orange region, where  $z + \vec{t} \cdot \vec{m} > 0$ . Re-arranging, we can view  $-z$  as the ‘bound’ on the linear function  $\vec{t} \cdot \vec{m}$  that separates the two regions.

### Exercises

- 3.4 Show that the set  $\mathcal{M}$  of measurement results—the image of  $\mathcal{S}$  from (3.27) under the mapping (3.28)—is a convex set. That is, show that if two sets of results  $\vec{m}_1$  and  $\vec{m}_2$  are both in  $\mathcal{M}$ , then so is any set of results of the form  $\vec{m}' = p\vec{m}_1 + (1 - p)\vec{m}_2$  for  $0 \leq p \leq 1$ .

### 3.1.7 Property estimation

It can sometimes be the case that we are less interested in estimating the full state  $\rho$  that led to the results  $\vec{m}$ , and more interested in knowing some property of it. If this property can be calculated by a linear function  $f(\rho)$ , such as energy or magnetisation, then we can find the range of values which are possible, by finding both the minimum and maximum value of this property that any quantum state  $\rho$  can have. To do this, we can modify the feasibility SDP (3.1) and introduce the objective function  $f(\rho)$ , which is either minimised or maximised.

As an example, we can estimate the maximum expected value of an unperformed measurement with observable  $\tilde{\mathcal{M}}$  by solving the following SDP

$$\text{maximise} \quad \text{tr}(\tilde{\mathcal{M}}\rho) \quad (3.29a)$$

$$\text{subject to} \quad \text{tr}(M_x\rho) = m_x \quad x = 1, \dots, N, \quad (3.29b)$$

$$\text{tr}(\rho) = 1, \quad (3.29c)$$

$$\rho \geq 0. \quad (3.29d)$$

By solving both this, and the analogous minimisation problem, we find the range of possible outcomes for the measurement  $\tilde{\mathcal{M}}$ , consistent with the set of measurement results observed. As previously, there are three regimes that can be encountered. If the measurements  $\tilde{\mathcal{M}}$  are tomographically complete, the feasible set is a unique state  $\mathcal{F} = \rho^*$ , and there will be a unique expectation value  $\tilde{m} = \text{tr}(\tilde{\mathcal{M}}\rho^*)$ . Conversely, if there is no solution (because the measurement results  $\vec{m}$  are inconsistent), the optimal value is  $\alpha^* = -\infty$ , signalling the infeasibility of the problem. Finally, when the measurements are consistent but not tomographically complete, we would expect there to be a range of values, all consistent with the measurement results.

In sections 3.1.1 and 3.1.2 we saw that it is possible to calculate the trace distance and fidelity to a target state  $\sigma$ . From the current perspective, we can view these as two further instances of property testing—of the state having the property of being  $\sigma$ . As was seen previously, even though the trace distance and fidelity are non-linear functions, both of these properties can nevertheless be estimated using semidefinite programming. It is possible to estimate other properties—specified by non-linear functions—using similar techniques.

### 3.2 The quantum marginal problem

In this final section we will now consider the quantum marginal problem. This problem is closely related to quantum state estimation, with the key difference being in the type of information given. In the previous sections of this chapter, we considered being given a set of measurement results, and were interested in estimating the quantum state—or properties of it—from this measurement data. We discussed in those sections the idea of tomographically complete data, i.e. data which is sufficient to uniquely determine the quantum state.

In the context of the quantum marginal problem, we will be interested in *multipartite* quantum states, comprising a number of subsystems. The assumption made now is that we have perfect knowledge of some of the subsystems—i.e. some of the *marginal* states, more commonly referred to as reduced density operators. This perfect knowledge can be thought of as being obtained by having tomographically complete data for these subsystems—i.e. by having performed a tomographically complete set of measurements, and having the corresponding measurement results. The basic problems of the quantum marginal problem are then to either determine the *global state* consistent with all of the marginals, or to estimate some property of this global state, given access only to the marginals.

We could now phrase everything just as was done above, in terms of measurement results. However, since the focus is now exclusively on situations where we have full knowledge of a number of subsystems, it is useful to adopt a more direct approach, and simply specify the reduced density operators of those subsystems. On the one hand, this is a conceptually cleaner way to approach the problem. On the other hand, it is an important lesson to realise that even in this formulation, we can still apply the techniques of semidefinite programming.

As a concrete example, let us consider the direct quantum analogue of the (classical) marginal problem considered in example 1.1. Therefore, consider a tripartite quantum system, with subsystems labelled by  $X$ ,  $Y$  and  $Z$ . Suppose that we have knowledge of the bipartite reduced density operators  $\rho_{XY}$ ,  $\rho_{XZ}$  and  $\rho_{YZ}$ , but not of the joint state  $\rho_{XYZ}$ . Consider that we want to determine whether there is any joint state consistent with the reduced density operators, and to find an example of one if it does. This can be cast as the following feasibility SDP:

$$\text{find } \sigma_{XYZ} \tag{3.30a}$$

$$\text{subject to } \text{tr}_Z(\sigma_{XYZ}) = \rho_{XY}, \tag{3.30b}$$

$$\text{tr}_Y(\sigma_{XYZ}) = \rho_{XZ}, \tag{3.30c}$$

$$\text{tr}_X(\sigma_{XYZ}) = \rho_{YZ}, \tag{3.30d}$$

$$\sigma_{XYZ} \geq 0, \quad \text{tr}(\sigma_{XYZ}) = 1. \tag{3.30e}$$

As with the state estimation problem, there are a number of interesting variants of this basic problem that can be considered. First, we can consider both trace distance

and fidelity estimation of the global state (or a marginal state) to a target state, in analogy to the problems studied in sections 3.1.1 and 3.1.2. We study these generalisations in exercises 3.5 and 3.6 respectively. Second, we can also consider the analogous problem of property estimation from section 3.1.7. This is studied in exercise 3.7 below.

We can also consider a problem which is closely related to the finite-statistics version of state estimation from section 3.1.3. Here we imagine that instead of knowing the bipartite reduced density operators exactly, they are only known approximately. One way to model this is to assume that the marginals need to be  $\epsilon$ -close to a fixed state, i.e. to demand

$$\|\sigma_{XY} - \rho_{XY}\|_1 \leq \epsilon, \quad (3.31)$$

where we have used the shorthand  $\sigma_{XY} = \text{tr}_Z(\sigma_{XYZ})$ , and similarly for  $\sigma_{XZ}$  and  $\sigma_{YZ}$ . We note that, just as when considering finite statistics,  $\epsilon$  is considered as being data which is specified in the problem—allowing us to impose either stricter or weaker constraints on how close the reduced density operators of  $\rho_{XYZ}$  need to be to the target states. Thus, we arrive at the following optimisation problem

$$\text{find } \sigma_{XYZ} \quad (3.32a)$$

$$\text{subject to } \|\sigma_{XY} - \rho_{XY}\|_1 \leq \epsilon, \quad (3.32b)$$

$$\|\sigma_{XZ} - \rho_{XZ}\|_1 \leq \epsilon, \quad (3.32c)$$

$$\|\sigma_{YZ} - \rho_{YZ}\|_1 \leq \epsilon, \quad (3.32d)$$

$$\sigma_{XYZ} \geq 0, \quad \text{tr}(\sigma_{XYZ}) = 1. \quad (3.32e)$$

As written, this is not an SDP, due to the non-linear inequality constraints (3.32b)–(3.32d). However, we can make use of the SDP characterisation of the  $\epsilon$  trace norm ball, as given in exercise 2.17, itself a small extension of the unit trace norm ball from equation 2.36. In particular, we arrive at

$$\text{find } \sigma_{XYZ} \quad (3.33a)$$

$$\text{s.t. } \sigma_{XY} - \rho_{XY} = \omega_{XY} - \zeta_{XY}, \quad \text{tr}(\omega_{XY} + \zeta_{XY}) = \epsilon, \quad \omega_{XY} \geq 0, \quad \zeta_{XY} \geq 0, \quad (3.33b)$$

$$\sigma_{XZ} - \rho_{XZ} = \omega_{XZ} - \zeta_{XZ}, \quad \text{tr}(\omega_{XZ} + \zeta_{XZ}) = \epsilon, \quad \omega_{XZ} \geq 0, \quad \zeta_{XZ} \geq 0, \quad (3.33c)$$

$$\sigma_{YZ} - \rho_{YZ} = \omega_{YZ} - \zeta_{YZ}, \quad \text{tr}(\omega_{YZ} + \zeta_{YZ}) = \epsilon, \quad \omega_{YZ} \geq 0, \quad \zeta_{YZ} \geq 0, \quad (3.33d)$$

$$\sigma_{XYZ} \geq 0, \quad \text{tr}(\sigma_{XYZ}) = 1. \quad (3.33e)$$

In order to emphasise the relationship between this formulation and (3.32), we have presented four constraints per line, which collectively replace the corresponding trace norm constraint from the former. Note also that we have had to introduce two new variables per constraint, thus arriving at a larger problem. Nevertheless, this

form is explicitly an SDP, and shows that it is possible to solve the analogue of the finite statistics problem for the quantum marginal problem. Finally, although we chose to place a constraint in terms of the trace norm, it is also possible in principle impose any distance-type constraint, as long as it can be expressed as an SDP. Examples of such include other norms, such as the operator norm, as well as the fidelity, both of which are left as exercises below.

Finally, we can also consider turning the problem from a feasibility SDP into a (standard) optimisation SDP. As always, there are numerous approaches that one can take to achieve this. Here we will consider a particularly simple approach which can be used when the target marginal states are *pure*. In this case, a relaxation of the marginal problem is to find a global state whose marginals have the largest average fidelity with the target pure marginals.

As a particular example, let us consider the analogue situation from exercise 1.9(c), where only two of the marginals are specified. Let us therefore assume that  $\rho_{XY} = |\psi_{XY}\rangle\langle\psi_{XY}|$  and  $\rho_{YZ} = |\psi_{YZ}\rangle\langle\psi_{YZ}|$ . The largest average fidelity that can be achieved with these two states is given by the following simple SDP

$$\text{maximise} \quad \frac{1}{2}(\langle\psi_{XY}|\sigma_{XY}|\psi_{XY}\rangle + \langle\psi_{YZ}|\sigma_{YZ}|\psi_{YZ}\rangle) \quad (3.34a)$$

$$\text{subject to} \quad \sigma_{XYZ} \geq 0, \quad \text{tr}(\sigma_{XYZ}) = 1. \quad (3.34b)$$

In exercise 1.9(c) it was shown that for the *classical* version of this problem, with only two pairwise marginals specified, as long as they were compatible—agreeing on the marginal distribution of the common random variable—then a global distribution always exists which perfectly reproduces the two marginals. In the quantum setting, interestingly, this is no longer the case. In particular, given two states  $|\psi_{XY}\rangle$  and  $|\psi_{YZ}\rangle$  such that  $\rho_Y = \text{tr}_X(|\psi_{XY}\rangle\langle\psi_{XY}|) = \text{tr}_Z(|\psi_{YZ}\rangle\langle\psi_{YZ}|)$ , in general there *will not* be a joint state of the three particles. The origin of this is *monogamy of entanglement*—a particle cannot simultaneously be highly entangled with two other particles, which introduces completely novel constraints into the marginal problem. As will be seen below in exercise 3.8, we can use the dual of (3.34) to show that a particle cannot simultaneously be in a pure entangled state with two other particles.

In chapter 5 we will return to an important variant of the marginal problem when studying the notion of a *k-symmetric extension*, a powerful tool in the theory of entanglement.

### Exercises

- 3.5 In this exercise we will consider problems involving finding the closest state to a target state—either the global state, or a marginal—in terms of the trace distance.
- (a) Consider a situation involving three particles, where we are given all of the pairwise marginals,  $\rho_{XY}$ ,  $\rho_{XZ}$  and  $\rho_{YZ}$ , and wish to estimate the trace distance between the closest compatible state  $\sigma_{XYZ}$  and a target global state  $\rho_{XYZ}$ .

- Write down the optimisation problem analogous to (3.4) that needs to be solved.  
*This problem will not be an SDP.*
- (b) Make use of (2.8) in order to re-express the optimisation problem from part (a) as an SDP.
- (c) Repeat the exercise from parts (a) and (b), assuming now instead that only the marginal states  $\rho_{XY}$  and  $\rho_{XZ}$  are specified, and that the goal is to estimate the trace distance between the closest compatible marginal state  $\sigma_{YZ}$  and a target marginal state  $\rho_{YZ}$ .
- 3.6 In this exercise we will repeat the same calculations as in the previous exercise, except instead of optimising the trace distance, we now optimise the fidelity.
- (a) Consider a situation involving three particles, where we are given all of the pairwise marginals,  $\rho_{XY}$ ,  $\rho_{XZ}$  and  $\rho_{YZ}$ , and wish to estimate the fidelity between the closest compatible state  $\sigma_{XYZ}$  and a target global state  $\rho_{XYZ}$ . Write down the optimisation problem that needs to be solved.  
*This problem will not be an SDP.*
- (b) Make use of (3.10) in order to re-express the optimisation problem from part (a) as an SDP.
- (c) Repeat the exercise from parts (a) and (b), assuming now instead that only the marginal states  $\rho_{XY}$  and  $\rho_{XZ}$  are specified, and that the goal is to estimate the fidelity between the closest compatible marginal state  $\sigma_{YZ}$  and a target marginal state  $\rho_{YZ}$ .
- 3.7 In this exercise we will consider *property estimation* in the context of the marginal problem. Consider that we are given the Hamiltonian  $H$  of three particles, and the three pairwise marginal states  $\rho_{XY}$ ,  $\rho_{XZ}$  and  $\rho_{YZ}$ . Our goal is to find the range of average energies that the system can have, consistent with these marginals.
- (a) Write down an SDP that evaluates the minimum possible average energy any global state  $\sigma_{XYZ}$  can have, given the Hamiltonian  $H$  and marginal states.
- (b) Write down an SDP that evaluates the maximum possible average energy any global state  $\sigma_{XYZ}$  can have, given the Hamiltonian  $H$  and marginal states.
- 3.8 In this exercise we will derive the dual SDP of (3.34) and use it to show that, when in a pure state, a qubit cannot simultaneously be entangled with two other qubits.
- (a) Write down the Lagrangian associated to the primal SDP (3.34), using  $M_{XYZ}$  and  $\mu$  as dual variables for the first and second constraint, respectively.
- (b) Identify the constraints that need to be satisfied by the dual variables in order that
- (i) The Lagrangian upper bounds the value of the primal objective function for all primal feasible variables.
  - (ii) The Lagrangian becomes independent of the primal variables.
- (c) Use parts (a) and (b) to show that, after solving for the slack variables, the dual SDP to (3.34) is

$$\text{minimise } \mu \tag{3.35a}$$

$$\text{subject to } \mu \mathbb{I} \geq \frac{1}{2}(|\psi_{XY}\rangle\langle\psi_{XY}| \otimes \mathbb{I}_Z + \mathbb{I}_X \otimes |\psi_{YZ}\rangle\langle\psi_{YZ}|). \tag{3.35b}$$

*This SDP can be solved explicitly, with optimal value given by*

$$\frac{1}{2} \|\Psi_{XY}\rangle\langle\Psi_{XY}| \otimes \mathbb{I}_Z + \mathbb{I}_X \otimes |\Psi_{YZ}\rangle\langle\Psi_{YZ}|\|_\infty.$$

- (d) For two projection operators  $\Pi_1$  and  $\Pi_2$ , the following bound can be shown to hold:

$$\|\Pi_1 + \Pi_2\|_\infty \leq 1 + \sqrt{\|\Pi_2\Pi_1\Pi_2\|_\infty}. \quad (3.36)$$

Writing the states  $|\Psi_{XY}\rangle$  and  $|\Psi_{YZ}\rangle$  in terms of their Schmidt decompositions,

$$|\Psi_{XY}\rangle = \sum_i \sqrt{p_i} |i_X\rangle |i_Y\rangle, \quad |\Psi_{YZ}\rangle = \sum_i \sqrt{q_i} |i_Y\rangle |i_Z\rangle,$$

use (3.36) to show that the optimum value of the dual SDP (3.35) is not larger than

$$\mu^* \leq \frac{1}{2} \left( 1 + \max_i \sqrt{p_i q_i} \right). \quad (3.37)$$

- (e) Explain why the answer to part (d) shows that a qubit cannot simultaneously be in a pure entangled state with two other particles.

### 3.3 Concluding remarks

In this chapter we began our exploration of applying semidefinite programming techniques to concrete problems in quantum information science. We mainly focused on the problem of quantum state estimation, which allowed us to study a variety of interesting features of SDPs. In particular, the main results described in this chapter are:

- **Quantum state estimation.** The first problem dealt with was determining the existence of a quantum state compatible with a set of measurement data. We introduced a few variants of this problem, in particular, focusing on different figures of merit, such as the trace distance and the fidelity. This demonstrated that problems involving non-linear objective functions can be cast as SDPs.
- **Double minimisation.** We showed that it is possible to cast problems involving double minimisation or double maximisation as SDPs—see (3.5).
- **Certificates of infeasibility.** When considering feasibility problems reformulated as optimisation problems, the dual variables of SDPs can often be viewed as providing certificates of infeasibility. This follows from the facts that (i) every feasibility SDP can be turned into an optimisation SDP in which a positive solution indicates that the original problem was infeasible; (ii) due to weak duality, the value of the objective function of the dual SDP lower bounds the optimal value of the primal SDP. This allows us to analytically certify infeasibility.

## 3.4 Further reading

- Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) <http://doi.org/10.1017/CBO9780511976667>

## 3.5 Advanced topics

### 3.5.1 The fidelity SDP

In this section we will derive the SDP formulation for fidelity as given in (3.10). Recall that for a general pair of quantum states  $\rho$  and  $\sigma$ , the fidelity is defined by

$$F(\rho, \sigma) = \|\sqrt{\rho} \sqrt{\sigma}\|_1^2. \quad (3.38)$$

Our starting point in this section will be *Uhlmann's theorem*, which gives an alternative expression for the fidelity in terms of *purifications* of  $\rho$  and  $\sigma$ . Recall that a purification of a (mixed) state  $\omega$  is a bipartite state  $|\chi\rangle$  such that

$$\text{tr}_B[|\chi\rangle\langle\chi|] = \omega, \quad (3.39)$$

where we label the systems as  $A$  and  $B$ .

Uhlmann's theorem then gives a classification of the fidelity in terms of the biggest overlap between any purification of  $\rho$  and  $\sigma$ , namely

$$F(\rho, \sigma) = \text{maximise } |\langle\psi|\phi\rangle|^2 \quad (3.40a)$$

$$\text{subject to } \text{tr}_B[|\psi\rangle\langle\psi|] = \rho, \quad (3.40b)$$

$$\text{tr}_B[|\phi\rangle\langle\phi|] = \sigma. \quad (3.40c)$$

Let us consider that we have found an arbitrary purification of  $\rho$  and an arbitrary purification of  $\sigma$ , which we denote by  $|\psi\rangle$  and  $|\phi\rangle$  respectively. Consider then the following state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle|0\rangle + e^{i\theta}|\phi\rangle|1\rangle), \quad (3.41)$$

where we have now introduced a third system, labelled  $C$ , taken to be a qubit, and an arbitrary phase factor  $e^{i\theta}$  which we will fix below.

The basic observation we make is that if  $|\psi\rangle$  and  $|\phi\rangle$  are *similar*—i.e. if they are close to being the same state, or have a large overlap  $|\langle\psi|\phi\rangle|$ —then the state  $|\Psi\rangle$  *cannot be very entangled*.

In particular, as will be seen later in chapter 5, the entanglement of a pure state can be determined by the reduced density operator of one subsystem. A state is entangled if and only if the reduced density operator (on any subsystem) is mixed. In our case, the reduced density operator of  $C$  is

$$\omega_C = \text{tr}_{AB}[|\Psi\rangle\langle\Psi|] = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + e^{-i\theta}\langle\phi|\psi\rangle|0\rangle\langle 1| + e^{i\theta}\langle\psi|\phi\rangle|1\rangle\langle 0|). \quad (3.42)$$

Let us now choose the angle  $\theta$  such that  $e^{i\theta}\langle\psi|\phi\rangle$  is real and nonnegative (and therefore equal to  $e^{-i\theta}\langle\phi|\psi\rangle$  and, moreover  $|\langle\psi|\phi\rangle|$ ). The purity of  $\omega_C$  is then seen to be

$$\text{tr}[\omega_C^2] = \frac{1}{2}(1 + |\langle\psi|\phi\rangle|^2). \quad (3.43)$$

This shows that when  $|\psi\rangle$  and  $|\phi\rangle$  are orthogonal, such that  $|\langle\psi|\phi\rangle| = 0$ , then the purity of  $\omega_C$  is minimal, since  $\omega_C = \frac{1}{2}\mathbb{I}$  is the maximally mixed state in this case. On the other hand, when  $|\langle\psi|\phi\rangle| = 1$ —meaning that they are the same state—then the purity of  $\omega_C$  is maximal, and indeed  $\omega_C = |+\rangle\langle+|$  is a pure state in this case. What this shows is that, as claimed, the entanglement of  $|\Psi\rangle$  depends upon the overlap of  $|\psi\rangle$  and  $|\phi\rangle$ , and can therefore be used to *measure* it.

We will now see how to use the above insight in order to derive (and interpret) the SDP for fidelity. Let us look instead at the reduced density operator  $\omega_{AC}$ ,

$$\omega_{AC} = \text{tr}_B[|\Psi\rangle\langle\Psi|], \quad (3.44a)$$

$$= \frac{1}{2}(\rho \otimes |0\rangle\langle 0| + \sigma \otimes |1\rangle\langle 1|) \quad (3.44b)$$

$$+ e^{-i\theta}\text{tr}_B[|\psi\rangle\langle\phi|] \otimes |0\rangle\langle 1| + e^{i\theta}\text{tr}_B[|\phi\rangle\langle\psi|] \otimes |1\rangle\langle 0|) \quad (3.44c)$$

where we used the fact that  $\text{tr}_B[|\psi\rangle\langle\psi|] = \rho$  and  $\text{tr}_B[|\phi\rangle\langle\phi|] = \sigma$ . Being a density operator, we know that  $\omega_{AC} \geq 0$ . Moreover, it can be seen that the trace of the Hermitian part of the off-diagonal block  $e^{-i\theta}\text{tr}_B[|\psi\rangle\langle\phi|]$  is

$$\text{tr}\left[\frac{e^{-i\theta}\text{tr}_B[|\psi\rangle\langle\phi|] + e^{i\theta}\text{tr}_B[|\phi\rangle\langle\psi|]}{2}\right] = |\langle\psi|\phi\rangle|. \quad (3.45)$$

Why is this relevant? Well, recall that, due to Uhlmann's theorem,  $|\langle\psi|\phi\rangle|$ , when maximised, is precisely  $\sqrt{F(\rho, \sigma)}$ . We have however just realised that  $|\langle\psi|\phi\rangle|$  is also the trace of the Hermitian part of the off-diagonal block of  $\omega_{AC}$ . This provides us with a way of obtaining an *upper bound* on the fidelity. The off-diagonal block  $e^{-i\theta}\text{tr}_B[|\psi\rangle\langle\phi|]$  can be treated as a *variable*, which we denote by  $\mathbf{Y} + i\mathbf{Z}$  (with  $\mathbf{Y} = \mathbf{Y}^\dagger$  and  $\mathbf{Z} = \mathbf{Z}^\dagger$  Hermitian operators) and then consider maximising the trace of  $\mathbf{Y}$  (the Hermitian part), subject to the constraint that  $\omega_{AC}$  is a valid density operator, namely

$$\sqrt{F(\rho, \sigma)} \leq \text{maximise } \text{tr}(\mathbf{Y}) \quad (3.46a)$$

$$\text{subject to } \begin{pmatrix} \rho & \mathbf{Y} + i\mathbf{Z} \\ \mathbf{Y} - i\mathbf{Z} & \sigma \end{pmatrix} \geq 0, \quad (3.46b)$$

where we have written  $\omega_{AC}$  as a block matrix, and have ignored the overall factor of  $\frac{1}{2}$ , which doesn't affect whether or not it is positive semidefinite. This is an upper bound, since we know that it is possible to take  $\mathbf{Y} + i\mathbf{Z} = e^{-i\theta}\text{tr}_B[|\psi\rangle\langle\phi|]$ , with  $|\psi\rangle$  and  $|\phi\rangle$  the optimal purifications of  $\rho$  and  $\sigma$  respectively (which achieve the fidelity

through Uhlmann's theorem), and with  $\theta$  such that  $e^{i\theta}\langle\psi|\phi\rangle$  is real. However, since we have relaxed the problem, and are maximising, there is no guarantee that this is the optimal solution, the maximum might be attained at a strictly larger number than the fidelity.

In order to show that this isn't the case, we can now proceed in the other direction, to show that  $\text{tr}(\mathbf{Y}^*) \leq \sqrt{F(\rho, \sigma)}$ . Let us assume that (3.46) has been solved, and that optimal variables  $\mathbf{Y}^*$  and  $\mathbf{Z}^*$  have been found. This in particular means that we have found a density operator

$$\omega_{AC}^* = \frac{1}{2}(\rho \otimes |0\rangle\langle 0| + \sigma \otimes |1\rangle\langle 1| + (\mathbf{Y}^* + i\mathbf{Z}^*) \otimes |0\rangle\langle 1| + (\mathbf{Y}^* - i\mathbf{Z}^*) \otimes |1\rangle\langle 0|). \quad (3.47)$$

Consider then a purification of  $\omega_{AC}^*$ , which we denote  $|\Psi^*\rangle$  (with the purifying system labelled  $B$ ). From this purification we can define two (normalised) states,

$$|\psi^*\rangle = \sqrt{2}(\mathbb{I}_{AB} \otimes \langle 0|_C)|\Psi^*\rangle, \quad |\phi^*\rangle = \sqrt{2}(\mathbb{I}_{AB} \otimes \langle 1|_C)|\Psi^*\rangle, \quad (3.48)$$

Crucially, these states can be seen to be purifications of  $\rho$  and  $\sigma$ . Indeed, we see that

$$\text{tr}_B[|\psi^*\rangle\langle\psi^*|] = 2\text{tr}_B[(\mathbb{I}_{AB} \otimes \langle 0|_C)|\Psi^*\rangle\langle\Psi^*|(\mathbb{I}_{AB} \otimes |0\rangle_C)], \quad (3.49a)$$

$$= 2[(\mathbb{I}_A \otimes \langle 0|_C)\omega_{AC}^*(\mathbb{I}_A \otimes |0\rangle_C)], \quad (3.49b)$$

$$= \rho, \quad (3.49c)$$

and similarly  $\text{tr}_B[|\phi^*\rangle\langle\phi^*|] = \sigma$ . (Note also that this confirms that  $|\psi^*\rangle$  and  $|\phi^*\rangle$  are normalised.) Now, the overlap between  $|\psi^*\rangle$  and  $|\phi^*\rangle$  is

$$|\langle\psi^*|\phi^*\rangle| = 2\langle\Psi^*|(\mathbb{I}_{AB} \otimes |0\rangle\langle 1|_C)|\Psi^*\rangle, \quad (3.50a)$$

$$= 2|\text{tr}[(\mathbb{I}_A \otimes |0\rangle\langle 1|_C)\omega_{AC}^*]|, \quad (3.50b)$$

$$= |\text{tr}(\mathbf{Y}^*) + i\text{tr}(\mathbf{Z}^*)|, \quad (3.50c)$$

$$= \sqrt{\text{tr}(\mathbf{Y}^*)^2 + \text{tr}(\mathbf{Z}^*)^2}. \quad (3.50d)$$

So, from Ulmann's theorem, since  $|\psi^*\rangle$  and  $|\phi^*\rangle$  are purifications of  $\rho$  and  $\sigma$ , we know that the fidelity  $F(\rho, \sigma)$  must be *at least*  $|\langle\psi^*|\phi^*\rangle|^2$ , and therefore we have the bound

$$\sqrt{F(\rho, \sigma)} \geq |\langle\psi^*|\phi^*\rangle| = \sqrt{\text{tr}(\mathbf{Y}^*)^2 + \text{tr}(\mathbf{Z}^*)^2}. \quad (3.51)$$

However, comparing with (3.46), we have  $\text{tr}(\mathbf{Y}^*) \geq \sqrt{F(\rho, \sigma)}$ . The only way that these two bounds can be satisfied is if  $\sqrt{F(\rho, \sigma)} = \text{tr}(\mathbf{Y}^*)$  and  $\text{tr}(\mathbf{Z}^*) = 0$ .

That is, this shows that in (3.46) the inequality can be replied by an equality, and that in fact this SDP precisely evaluates to the fidelity between  $\rho$  and  $\sigma$ .

The derivation is moreover interesting since it sheds light on how to interpret the SDP. We can view the objective function as maximising the entanglement of a state

of the form (3.41), which entangles purifications of  $\rho$  and  $\sigma$ . Only if the states have a small fidelity (meaning they are close to being orthogonal) can there exist purifying states that then can be superposed and generate a large amount of entanglement. When the states have a large fidelity, meaning they are similar, it is not possible to find purifications of them which generate much entanglement by superposing them.

This can be viewed as a type of *trade-off* relation, between how similar states are, and how much their purifications can be entangled with an auxiliary system, and shows that the fidelity quantifies this trade-off.