Aspects of Entanglement

by

Robert W. Spekkens

A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy
Graduate Department of Physics
University of Toronto

Copyright © 2001 by Robert W. Spekkens
The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L’auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L’auteur conserve la propriété du droit d’auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-63757-3
Abstract

Aspects of Entanglement

Robert W. Spekkens
Doctor of Philosophy
Graduate Department of Physics
University of Toronto
2001

We present a theoretical study of entanglement in selected topics from quantum cryptography, Bose-Einstein condensation and the interpretation of quantum mechanics. First, we consider the two-party cryptographic task known as bit commitment. For specific types of bit commitment protocols, we determine the optimal cheating strategy for one of the parties, and identify the cases wherein the cheater must have the ability to generate entanglement. We proceed to determine the maximum degree of security that can be achieved against each party given various restrictions on the form of the protocol. In particular, we identify a family of protocols wherein there is a linear trade-off between the maximum probabilities of each party cheating successfully. Next, we consider the fragmentation of a Bose-Einstein condensate, wherein multiple single-particle wavefunctions acquire a macroscopic occupation number. We demonstrate that for atoms with weak repulsive inter-particle interactions trapped in a double-well potential, one can achieve various degrees of squeezing in the relative number of atoms between the wells by varying the height of the central barrier and allowing the system to relax to the ground state. This constitutes a technique for generating entanglement between a pair of localized atomic modes. Finally, we propose a modal interpretation of quantum mechanics based on a novel choice of preferred decomposition for a multi-partite entangled state: from among all decompositions containing only product states, it is the one for which the coefficients squared have the smallest Shannon entropy. This proposal is shown to compare favorably
with those that make use of the bi-orthogonal decomposition, particularly in the extent to which it provides a solution to the quantum measurement problem.
## Contents

1 Introduction 1

1.1 Aspects of entanglement in quantum bit commitment ................. 4
1.2 Aspects of entanglement in the fragmentation of Bose-Einstein condensates 8
1.3 Aspects of entanglement in modal interpretations of quantum mechanics 10

2 Optimizing coherent attacks in generalizations of the BB84 quantum bit commitment protocol 14

2.1 Introduction ........................................ 14
2.2 Bit Commitment ........................................ 17
   2.2.1 Preliminaries ................................. 17
   2.2.2 Types of security ............................. 17
   2.2.3 Generalizations of the BB84 BC protocol .............. 18
2.3 Convex decompositions of a density operator ........................ 20
   2.3.1 Definition and properties of convex decompositions .............. 20
   2.3.2 The connection between convex decompositions and POVMs ... 22
   2.3.3 The significance of convex decompositions for coherent attacks ... 23
2.4 The nature of the optimization problem ............................ 26
2.5 Results for general protocols .................................. 27
   2.5.1 The connection to state estimation .................... 27
   2.5.2 The support of the optimal density operator ............... 29
2.5.3 Conditions for unveiling with certainty .......... 30
2.6 Results for qubit protocols .......................... 31
  2.6.1 The Bloch ball representation ...................... 31
  2.6.2 The conditions under which Alice can unveil the bit of her choosing with certainty .................. 36
  2.6.3 Optimizing over the convex decompositions of an arbitrary but fixed density operator .................. 37
  2.6.4 Optimizing over density operators .................. 40
2.7 Applications of the results .......................... 45
2.8 Conclusions ........................................... 51

3 Degrees of bindingness and concealment in quantum bit commitment protocols 53
  3.1 Introduction .......................................... 53
  3.2 Degrees of concealment and bindingness ................ 54
  3.3 BC protocols ......................................... 58
  3.4 Measures of distinguishability for density operators .......... 62
  3.5 Optimizing over all BC protocols ........................ 64
  3.6 Optimizing over Alice-supplied BC protocols ............... 68
    3.6.1 Optimal degrees of concealment and bindingness .......... 68
    3.6.2 Optimal trade-off relations ........................ 73
  3.7 Significance for coin tossing .......................... 75
  3.8 Conclusion ........................................... 76

4 Spatial fragmentation of a Bose-Einstein condensate in a double-well potential 78
  4.1 Introduction .......................................... 78
  4.2 The Model ............................................. 81
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1</td>
<td>The basic approach</td>
<td>81</td>
</tr>
<tr>
<td>4.2.2</td>
<td>A restricted variational principle</td>
<td>84</td>
</tr>
<tr>
<td>4.2.3</td>
<td>The regime of nearly non-interacting particles</td>
<td>86</td>
</tr>
<tr>
<td>4.2.4</td>
<td>Measures of the degree of fragmentation</td>
<td>88</td>
</tr>
<tr>
<td>4.3</td>
<td>Analytic Approximations and Numerical Solutions</td>
<td>89</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Continuum approximation</td>
<td>90</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Two-coefficient approximation</td>
<td>93</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Numerical solutions</td>
<td>97</td>
</tr>
<tr>
<td>4.4</td>
<td>Discussion</td>
<td>99</td>
</tr>
<tr>
<td>4.4.1</td>
<td>The experimental signature of fragmentation</td>
<td>99</td>
</tr>
<tr>
<td>4.4.2</td>
<td>Finite temperatures</td>
<td>102</td>
</tr>
<tr>
<td>4.5</td>
<td>Conclusions</td>
<td>102</td>
</tr>
<tr>
<td>5</td>
<td>A modal interpretation of quantum mechanics based on a principle of</td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>entropy minimization</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>105</td>
</tr>
<tr>
<td>5.2</td>
<td>A preferred decomposition based on a principle of entropy minimization</td>
<td>111</td>
</tr>
<tr>
<td>5.3</td>
<td>The minimal entropy proposal as a modal interpretation</td>
<td>117</td>
</tr>
<tr>
<td>5.4</td>
<td>The quantum measurement problem</td>
<td>121</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Single measurements</td>
<td>122</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Sequences of measurements</td>
<td>130</td>
</tr>
<tr>
<td>5.5</td>
<td>The Faithfulness criterion</td>
<td>133</td>
</tr>
<tr>
<td>5.6</td>
<td>Conclusions</td>
<td>136</td>
</tr>
<tr>
<td>6</td>
<td>Conclusions and future directions</td>
<td>141</td>
</tr>
<tr>
<td>A</td>
<td>Proof of results of section 2.6.3</td>
<td>147</td>
</tr>
<tr>
<td>B</td>
<td>Proof of results of section 2.6.4</td>
<td>150</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

When two systems, of which we know the states by their respective representatives, enter into temporary physical interaction due to known forces between them, and when after a time of mutual influence the systems separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives (or ψ-functions) have become entangled. (Erwin Schrödinger, 1935)

A pure state of a composite quantum system is said to be entangled if it cannot be written as a product of pure states of its component systems. This feature of quantum states has no analogue in classical mechanics. Indeed, some physicists have gone so far as to claim that entanglement is the quintessential feature of quantum mechanics, as in the quote provided above.

The concept of entanglement first captured the attention of the physics community with the publication of the seminal paper of Einstein, Podolsky and Rosen [1], wherein it plays a key role in an argument for the incompleteness of quantum mechanics. Shortly thereafter, it made another significant appearance in an article by Schrödinger [2] describ-
ing the thought experiment with the eponymous cat, which first introduced the quantum measurement problem. Its reputation as the 'première' non-classical effect was consolidated in 1964 with the demonstration by John Bell [3] that the correlations predicted by certain entangled states were inconsistent with the assumption of local realism. Since then, experimental evidence has ruled in favor of quantum mechanics and against local realism.

Although entanglement was for a time best known for its foundational significance, more recently it has become celebrated as a valuable resource with which the efficiency of various tasks can be improved beyond what could be achieved classically. Examples of such tasks include high-precision interferometry [4], clock synchronization [5], and lithography [6], as well as a multitude of tasks in cryptography, communication and computation [7]. Moreover, there are many more "fundamental" tasks which do not by themselves have any obvious application, but which constitute a primitive for others which do, for instance, quantum teleportation [8].

The realization that it constitutes a physical resource, like energy or entropy, has greatly increased our understanding of entanglement. For instance, one can quantify the entanglement of a particular state by the degree to which one can perform various tasks using that state. The quantification of entanglement has been, and continues to be, the subject of a vast amount of research [9].

Although we now have a reasonable understanding of how to quantify the entanglement of bi-partite pure states, we still have little understanding of how to do so for bi-partite mixed states. Moreover, we have almost no idea of how to do so for states entangled over more than two systems. In addition, although the number of tasks that rely for their success or efficiency on quantum mechanics continues to grow, we have yet to really understand how this greater success or efficiency is achieved, and in particular to what extent entanglement is necessary. Finally, despite great experimental and theoretical progress in the field of quantum theory over the last three-quarters of a century, there
remains a remarkable lack of consensus on the implications of the theory, in particular the concept of entanglement, to our scientific world view. These facts support the notion that, as a community, our understanding of entanglement remains quite poor.

In this thesis, we consider entanglement from both of the perspectives described above: as a resource to physical and information-theoretic tasks and as a critical piece of the quantum interpretation puzzle. Our results contribute to answering general questions about entanglement such as: “What tasks can be performed more successfully using entanglement than could be accomplished otherwise?”, “How can one generate states of varying degrees of entanglement in practice?”, and “How can one interpret macroscopic objects in entangled states as having definite properties?” In chapters 2 and 3 we consider entanglement as a resource for cheating strategies in a cryptographic protocol known as quantum bit commitment. In chapter 4, we study a way of generating states of varying degrees of entanglement between spatially separated modes of a Bose-Einstein condensate. In chapter 5, we propose a ‘canonical’ decomposition for multi-partite entangled states from which we build a realist interpretation of quantum mechanics that has some success in resolving the quantum measurement problem. In chapter 6, we present our conclusions and discuss some promising research directions.

In the remainder of this introduction, we present an overview of the topics covered by the thesis, summarizing our results for each. The contents of chapter 4 have been published in Physical Review A [10], the contents of chapter 5 are forthcoming in Foundations of Physics [11], and the contents of chapters 2 and 3 have been submitted for publication in Quantum Information & Computation [12] and Physical Review A [13] respectively.
1.1 Aspects of entanglement in quantum bit commitment

Suppose Alice and Bob wish to play a game wherein Alice wins if she can correctly predict which of two mutually exclusive events will occur and Bob wins if she cannot. One way to play the game would be for Alice to tell Bob her prediction before the events in question. There are situations, however, where this is inappropriate. For instance, Bob might be able to influence the relative probability of the events in question (indeed, which of these events occurs might be entirely up to Bob). In such cases, Alice wants Bob to know as little as possible about her prediction until some time after the occurrence of one of the events. Of course, Bob will still want to receive some sort of ‘token’ of Alice’s prediction prior to the events in question, since otherwise Alice could always claim to have won the game. Thus, Alice and Bob would like a cryptographic protocol which forces Alice to ‘commit’ herself to a bit (which encodes her prediction), while ensuring that Bob can find out as little as possible about this bit until the time that Alice unveils it to him. This is a bit commitment (BC) protocol. In addition to the task of prediction described above, BC appears as a primitive in many other cryptographic tasks, such as coin tossing [14], quantum gambling [16], bit escrow [17] and two-party secure computation [18], and is therefore particularly significant.

A simple example of an implementation of BC proceeds as follows. Alice writes a ‘0’ or a ‘1’ on a piece of paper, and locks this in a safe. She then sends the safe to Bob, but keeps the key. When it comes time to unveil her commitment, she sends the key to Bob, who opens the safe and discovers the value of the bit. This protocol binds Alice to the bit she chose at the outset since she cannot change what is written on the piece of paper after she submits the safe to Bob. However, it only conceals the bit from Bob if he is unable to pick the lock, or force the safe open, or image the contents of the safe.

One would prefer a protocol that is secure even if Bob has unlimited resources, that
is, a protocol whose security depends only on the laws of physics. Such a protocol is said to be unconditionally secure. It was thought for a time that one could achieve this with the use of quantum systems; however, this turned out to be mistaken. To see why, we consider a simple example, namely, the very first proposal for a quantum mechanical implementation of BC, which was made by Bennett and Brassard in 1984 [19]. We refer to it as the BB84 BC protocol (note that this protocol was recognized by its authors to be insecure against Alice).

Suppose Alice submits a qubit (i.e. a 2-level quantum system) to Bob to encode her commitment. To commit to a bit 0, she prepares the qubit in a state chosen uniformly from the set \{\ket{0}, \ket{1}\}, while to commit to a bit 1, she chooses from the set \{\ket{+}, \ket{-}\}, where \ket{\pm} \equiv (\ket{0} \pm \ket{1})/\sqrt{2}. No measurement Bob can do is able to distinguish these two possibilities; thus, he cannot gain any information about Alice's commitment. When Alice wishes to unveil her commitment, she tells Bob which state she submitted, and Bob can do a measurement of the projector onto this state to verify her honesty. If Alice tries to convince Bob that she submitted a state drawn from the opposite set - for instance, that she submitted \ket{+} when in fact she submitted \ket{0} - then her probability of passing his test is only 1/2. The BB84 BC protocol demands that Alice repeat her commitment for \(N\) qubits, that is, that Alice either chooses each qubit's state uniformly from \{\ket{0}, \ket{1}\} or uniformly from \{\ket{+}, \ket{-}\}. Clearly, in this case her probability of passing Bob's test when she lies about her commitment is \(1/2^N\). Thus, with respect to strategies wherein Alice cheats by lying about her commitment, such a protocol appears to be secure against Alice.

However, Alice has another cheating strategy available to her. Prior to submitting a qubit to Bob, she can entangle it with a qubit that she keeps in her possession. Specifically, she prepares the two in the entangled state \((\ket{0}\ket{1} - \ket{0}\ket{1})/\sqrt{2}\). Given that this state can also be written as \((\ket{+}\ket{-} - \ket{-}\ket{+})/\sqrt{2}\), it is clear that by measuring the \{\ket{0}, \ket{1}\} basis or the \{\ket{+}, \ket{-}\} basis on the qubit in her possession, she projects the
qubit in Bob’s possession into the \{ |0\rangle, |1\rangle \} basis or the \{ |+\rangle, |−\rangle \} basis respectively. Moreover, the binary outcome of her measurement will be perfectly anti-correlated with the state of Bob’s qubit. So Alice knows precisely which state to announce to Bob. Using this strategy, she can delay choosing which bit she wants to unveil until the end of the protocol, and always succeed at convincing Bob that she initially submitted that bit. This is called a ‘coherent’ or ‘EPR’ attack.

We see therefore that an ability to generate entanglement allows Alice to increase her probability of unveiling the bit of her choosing from \(1/2^N\) to unity! This insecurity against Alice is in fact generic. In seminal papers on the subject, Mayers [20], and independently, Lo and Chau [21], demonstrated that in any BC protocol where Bob’s information gain is negligible, Alice’s probability of successfully cheating can be made arbitrarily close to unity if she uses entanglement.

Nonetheless, one can still ask: is it possible to devise a protocol wherein Bob can get non-negligible information about Alice’s commitment, but Alice cannot alter her commitment at will? It turns out that such a protocol is possible. The simplest example is as follows. Alice submits the state \(|0\rangle\) to commit to 0, and the state \(|+\rangle\) to commit to 1. Since \(|0\rangle\) and \(|+\rangle\) are non-orthogonal, there are measurements Bob can perform which give him some information about which bit Alice committed. Moreover, if Alice submits \(|0\rangle\) and later tries to pass the test for \(|+\rangle\), she has some probability of succeeding.

There are in fact many other more complicated protocols that also have this feature. The existence of such protocols means that there are many interesting questions left to be answered. First, for an arbitrary protocol, what are Bob and Alice’s optimal cheating strategies? Second, what protocol is optimal in the sense of minimizing the amount that Bob and Alice can cheat?

Consider the optimization of cheating strategies. The diversity of possible protocols is such that we do not consider an arbitrary protocol, but rather restrict our attention to two simple classes. Protocols in the first class are just like the BB84 BC protocol
presented above except that the set of states from which an honest Alice chooses can have an arbitrary number of non-orthogonal elements, and the probabilities with which they are chosen need not be equal. Protocols in the second class are of a novel form. Alice prepares a pair of systems in one of two entangled states depending on the bit she wishes to commit. She then submits one member of the pair to Bob as the 'encoding' of her bit. When Alice unveils her bit, she must prove her honesty to Bob by supplying the other member of the entangled pair.

It turns out that optimizing Bob's cheating strategy is straightforward in these protocols, since all Bob can do is attempt to determine the state of the system Alice submitted to him, and the solution to the problem of optimal state estimation is well-known. Thus it is the problem of optimizing Alice's cheating strategy which is our focus.

In chapter 2 we provide an analytic solution for Alice's optimal attack in certain types of generalized BB84 BC protocols, specifically, protocols that can be implemented using a single qubit and involving at most four states. We demonstrate that Alice must in general make use of entanglement in her optimal strategy. In chapter 3 we provide a complete analytic solution for all purification BC protocols. The optimal coherent attack in this case involves Alice preparing an entangled state that 'interpolates' in a particular way between the entangled states associated with honest commitments of 0 and 1.

The second task we set for ourselves above was to optimize the degree of security that can be achieved in BC. Since Alice seeks for Bob to find out as little as possible about the bit committed, we call the degree of security against Bob the degree of concealment. Similarly, since Bob wishes for Alice to be unable to change her commitment, we call the degree of security against Alice the degree of bindingness. These quantities are defined precisely in chapter 3.

The Mayers-Lo-Chau theorem, mentioned previously, demonstrates that no protocol yields complete concealment and complete bindingness. However, there are protocols that are partially concealing and partially binding, and as we show in chapter 3, there is
in fact a trade-off between these two quantities - if the degree of bindingness is increased, the degree of concealment must decrease. Our goal therefore is to determine the maximum degree of bindingness that can be achieved for every degree of concealment. In other words, we seek to identify the best achievable trade-off between concealment and bindingness.

In chapter 3, we identify an upper bound on the maximum degree of bindingness that can be achieved for every degree of concealment. For instance, we find that for a ‘fair’ protocol - wherein the degree of concealment is equal to the degree of bindingness - Alice and Bob cannot make their probability of successfully cheating any greater than about 0.69. Unfortunately, we are unable to determine whether or not this bound is saturable. We do however solve the optimization problem under various restrictions on the form of the BC protocol. Our most significant result is that in a large class of BC protocols - which includes the generalized BB84 BC protocols, the purification BC protocols and many others - the best achievable trade-off between concealment and bindingness is linear. For example, in the case of a fair protocol, Alice and Bob each have at most a probability of 0.75 of successfully cheating. We conjecture that this linear trade-off is in fact the optimal trade-off from among all BC protocols.

1.2 Aspects of entanglement in the fragmentation of Bose-Einstein condensates

It is customary to approximate the many-body ground state of a spinless Bose-Einstein condensate by a Hartree-Fock state, wherein all the particles occupy the same single-particle wavefunction. In contrast, a fragmented condensate is one wherein two or more orthogonal single-particle wavefunctions have a macroscopic occupation. Nozières [22] has argued that for bosons with repulsive inter-particle interactions, fragmentation is made energetically unfavorable due to the large exchange energy of a fragmented state.
However, in a non-uniform trapping potential the overlap between different spatial modes can become small and consequently the exchange energy is less significant. In such cases, fragmentation into different spatial modes may occur if the interaction energy benefit of separating the bosons outweighs the kinetic energy cost. This simple argument for the possibility of fragmentation is presented in detail in Appendix D.

In chapter 4, we consider a zero-temperature gas of atoms with repulsive inter-particle interactions confined to a double-well potential. In particular, we investigate the change in the ground state as the height of the central barrier of the potential is varied. We show that states which have entanglement between the occupation numbers of the spatial modes associated with each well yield a better approximation of the fully interacting ground state than a Hartree-Fock state. In particular, we demonstrate that the variance in relative occupation number of the two modes is squeezed to various degrees as the barrier height is varied.

The ability to generate variable degrees of entanglement of this sort has significant applications. In particular, it is likely to be useful in attempts to increase the precision of phase estimation in atom interferometry [4], which is the basis of many high-precision measurement devices such as detectors for rotation, acceleration and even gravitational waves.

The details of our analysis are as follows. Using a restricted variational principle, we determine the equation that must be satisfied by the many-body ground state. We provide both approximate analytic as well as numerical solutions of our model in the regime where the inter-particle interactions can be treated perturbatively. The degree of fragmentation at a given barrier height is characterized by the degrees of first-order and second-order spatial coherence across the barrier, and can be measured in a certain type of interference experiment which we describe. We present chapter 4 in its published form [10].
1.3 Aspects of entanglement in modal interpretations of quantum mechanics

In an operational approach to quantum mechanics, theoretical predictions take the form 'if such-and-such a measurement is made after such-and-such a preparation, such-and-such an outcome will be found with such-and-such a probability'. In contrast, a realist interpretation is an attempt to understand quantum mechanics as making stronger claims of the form 'such-and-such a variable has such-and-such a value with such-and-such a probability'. There are many reasons for being dissatisfied with a strictly operational approach [23]. We do not discuss these here except to suggest, with Einstein, that to settle for operationalism would have the result that "physics could only claim the interest of shopkeepers and engineers" [24].

The goal of a realist interpretation is to provide an observer-independent description of the predictions of the theory. The variables that receive well-defined values within such a description have been called 'elements of reality' by Einstein, Podolsky and Rosen [1], and 'be-ables' by Bell [26]. We will simply refer to them as determinate variables. Within this approach, one assigns a property to a system by assigning a value to a determinate variable. In order to provide a complete specification of properties for a system it is therefore necessary to specify both a set of determinate variables and a set of values for these variables.

The standard approach to assigning properties, called the 'orthodox' approach, is to assume that a variable is determinate if and only if it is associated with an operator for which the state vector is an eigenstate, in which case its value is the corresponding eigenvalue. Given the applicability of quantum mechanics over a broad range of energy scales and levels of compositeness of the systems investigated, it seems reasonable to suppose that the theory is universally applicable, or at the very least applicable on the scale of macroscopic objects, such as measurement devices. However, if one attempts to
provide a realist description of such devices using the orthodox approach, one immediately encounters a serious difficulty known as the quantum measurement problem.

This can be illustrated as follows. Given a simple model of the interaction between the object of investigation and the measurement apparatus, one finds, in an ideal measurement, a final state of the form $\sum_k c_k |\varphi_k\rangle |A_k\rangle$ where the $|\varphi_k\rangle$ are eigenvectors of the variable measured and the $|A_k\rangle$ are a set of orthogonal vectors describing the apparatus indicating the different possible outcomes of the measurement. In order for the apparatus to be assigned the property of indicating a particular outcome, a 'pointer observable' of the form $\sum_k a_k |A_k\rangle \langle A_k|$ (with non-degenerate $a_k$) must be determinate. However, if more than one of the coefficients $c_k$ is non-zero, $\sum_k c_k |\varphi_k\rangle |A_k\rangle$ is not an eigenstate of $\sum_k a_k |A_k\rangle \langle A_k|$ and thus the orthodox approach fails to predict that the apparatus indicates a definite outcome at the end of the measurement. This is the quantum measurement problem [27].

The root of the problem is that the apparatus is entangled with the object system. Had the two been in a product state of the form $|\varphi_k\rangle |A_k\rangle$, then the apparatus would receive the appropriate properties. Thus, it has been proposed [28] that one should attempt to find a modification of the formalism of quantum theory that incorporates a non-unitary dynamics for the state vector (often called a 'collapse') which would ensure that the final state vector is $|\varphi_k\rangle |A_k\rangle$ with probability $|c_k|^2$. Ideally, this modification would only affect the dynamics of macroscopic objects, but given that 'macroscopicness' is a matter of degree, it is likely that there will be consequences for microscopic and mesoscopic dynamics as well. The fact that no experiment at these scales has yet to provide any evidence for a non-unitary evolution law has led many to favor a different response to the measurement problem, namely, that it is the orthodox approach to property ascription which should be rejected. What is proposed is that the state vector does not fix the actual property ascription. Rather, the state vector merely describes the set of possible property ascriptions. Since the logic of possibility is modal logic, realist no-
collapse interpretations of this type have been called modal interpretations of quantum mechanics [29][32][33][25].

There are many variations upon this approach. In the approach we adopt, the actual property ascription at a given time is still fixed by applying the orthodox rule to a vector in Hilbert space - but not the vector which obeys Schrödinger's equation. It is fixed instead by a new vector, essentially a hidden variable which is added to the formalism. We call it the property state vector. The vector which appears in Schrödinger's equation, which we call the dynamical state vector, is left with two roles to play. First, it specifies the dynamics of the property state vector. Secondly, it determines the set of possibilities for the property state vector. More specifically, at every time, the interpretation specifies a decomposition of the dynamical state vector into some orthogonal set of states. We call this the preferred decomposition. The property state vector is always one of the elements of the preferred decomposition, and evolves by a stochastic dynamics in such a way that the probability of it being a particular element is simply the modulus squared of its amplitude in the decomposition. Thus, every modal interpretation of this type must specify both a rule for identifying the preferred decomposition and a dynamical law for the property state vector.

So, in the simple example provided above, if the preferred decomposition at the end of the measurement contained the states \{ |\varphi_k \rangle | A_k \rangle \}, then the property state vector would be \( |\varphi_k \rangle | A_k \rangle \) with probability \( |c_k|^2 \), and the apparatus would have the property of indicating outcome \( k \). Note however that for an interpretation to be satisfactory, the preferred decomposition cannot be simply specified by fiat. Rather, it must be specified in the formalism as a mathematical rule. It turns out that there is in fact a simple rule which yields the desired result in the example considered here (assuming the \( c_k \) are non-degenerate). The rule is to adopt the bi-orthogonal decomposition as preferred.

This decomposition (which is defined precisely in chapter 5) has been used for the purposes of interpretation by many authors [34][35][36]. The idea has been refined over
the years, and is the seed of several modern modal interpretations [37],[38],[39]. These proposals have several outstanding problems. In particular, due to the behaviour of the bi-orthogonal decomposition when its coefficients pass near degeneracies, macroscopic objects may not always receive the appropriate properties. This suggests that this decomposition is ultimately inappropriate as the preferred decomposition.

In chapter 5 of this thesis, we propose a new choice of preferred decomposition, namely, a particular generalization of the bi-orthogonal decomposition to multi-partite systems. Our suggestion is to use the product decomposition for which the set of coefficients squared has the smallest entropy. To identify this decomposition, we must perform a variation over the set of all product decompositions. The main technical result of this chapter is the solution of this variational problem for a particular class of state vectors. Using these results, we are able to consider the merits of our proposal. Within models of measurement that are more realistic than the one presented above, and indeed, more realistic than the standard models which are considered in this context, we find that our proposal solves the measurement problem for a large class of measurements and does not obviously suffer from the same difficulties near degeneracies as the aforementioned proposals. Finally, our proposal has the distinction of providing, for a large class of measurements, a very intuitive account of measurement outcomes that occur with certainty: these simply reveal pre-existing properties of the system under investigation.
Chapter 2

Optimizing coherent attacks in generalizations of the BB84 quantum bit commitment protocol

2.1 Introduction

This chapter focuses on a particular class of quantum BC protocols, which we call generalized BB84 BC protocols [19]. Within such protocols, an honest Alice commits to a bit 0 by choosing a state randomly from a specified set of states, and by subsequently sending a system prepared in this state to Bob. She commits to a bit 1 by choosing the state from a different set. At the end of the protocol she reveals to Bob which state she submitted and Bob measures the projector onto this state to verify Alice's claim.

Bob can cheat in such a protocol by performing a measurement on the systems submitted to him by Alice, prior to Alice revealing her commitment. The measurement that maximizes his probability of correctly estimating Alice's commitment can be determined from the well-known theory of state estimation [40][41].

Alice can cheat by preparing the system she initially submits to Bob in a state different
from the ones specified by the protocol, in particular, by entangling this system with an ancilla system that she keeps in her possession, and by later performing a measurement on the ancilla and choosing the state which she announces to Bob based on the outcome of this measurement. This has been called a coherent attack, since in general such an attack requires Alice to maintain the coherence between the different possibilities in the random choice the protocol asks her to make. It has also been called an EPR-type attack, since in the original BB84 BC protocol, the optimal entangled state for Alice to prepare is the EPR state. The problem of determining the coherent attack that maximizes Alice's probability of successfully cheating has remained open to date. It is the goal of this chapter to begin to answer this question.

It should be noted that coherent attacks are important in many quantum cryptographic tasks between mistrustful parties - such as coin tossing [14], cheat sensitive bit commitment [15], quantum gambling [16], and bit escrow [17] - wherein a type of bit commitment often appears as a subprotocol. Understanding how to optimize coherent attacks is therefore important for settling questions about the degree of security that can be achieved for such tasks.

We summarize here the main results of this chapter. The last four apply only to protocols that can be implemented using a single qubit.

- We explain coherent attacks in terms of a theorem about entanglement due to Hughston, Jozsa and Wootters [42].

- We demonstrate that the problem of finding the optimal coherent attack for a fixed submitted state can be mapped onto a problem of state estimation.

- We show that the optimal state for a cheating Alice to submit has a support in the span of the states that an honest Alice chooses from.

- We provide a simple geometrical picture on the Bloch sphere of coherent attacks. In addition to being useful for building one's intuitions about such attacks, this
provides a convenient formalism within which to solve the optimization problem, as well as a geometrical criterion for whether or not Alice can cheat with probability 1 in a given protocol.

- We find analytic expressions for the optimal cheating strategy in the case where the sets of states that an honest Alice chooses from each have no more than two elements.

- Using these results, we determine Alice’s optimal coherent attack in a BC protocol that was proposed by Aharonov et al. [17]. Our result provides a tight upper bound on Alice’s probability of unveiling whatever bit she desires, improving upon the best previous known upper bound. This allows us to determine, for this protocol, the trade-off relation between the degree of concealment and the degree of bindingness. We show that the same trade-off relation can be achieved with several other protocols.

- Finally, our results allow us to determine Alice’s optimal coherent attack in a new type of generalized BB84 BC protocol wherein the trade-off relation between concealment and bindingness is better than can be achieved with the protocol of Aharonov et al.

This chapter is organized as follows. In section 2.2, we introduce some terminology, define degrees of security, and describe in detail generalized BB84 BC protocols. In section 2.3, we introduce the notion of a convex decomposition of a density operator, review its properties, and demonstrate its significance for coherent attacks. In section 2.4, we formulate the optimization problem to be solved. Results for protocols involving systems of arbitrary dimensionality and for protocols involving qubits are presented in sections 2.5 and 2.6 respectively. Applications of these results are presented in section 2.7, and section 2.8 contains our concluding remarks.
2.2 Bit Commitment

2.2.1 Preliminaries

We begin by introducing some useful terminology for describing a BC protocol. The point in the protocol when Alice submits the system encoding her bit to Bob is called the commitment phase. The point in the protocol where Alice announces to Bob the state she submitted, and Bob measures the projector onto this state is called the unveiling phase. The time between we call the holding phase. If Alice passes Bob's test, then the result of the protocol is '0' or '1', depending on whether the state Alice has announced falls into the set associated with bit 0 or the set associated with bit 1; otherwise, the result is 'fail'.

If Alice cheats, she typically has some probability of failing Bob's test, however she will not always be caught when she cheats. Thus, it can happen that the result of the protocol is 'b' even though Alice cheated and did not follow the honest strategy for committing a bit b. Indeed, Alice can, by cheating, change the relative probability of the '0' and '1' results by actions taken after the commitment phase. Since Alice can influence the result of the protocol by her choice of cheating strategy, we shall say that 'Alice unveils bit b' whenever the result 'b' occurs.1

2.2.2 Types of security

To define the security of a BC protocol, one needs to quantify the notions of concealment against Bob and bindingness against Alice. In this thesis, we focus upon the probability that Bob can, prior to the beginning of the unveiling phase, correctly estimate Alice's commitment (given that Alice is honest), and the probability that Alice can, after the end

---

1 It is important to remember that within our terminology 'Alice unveiling bit b' implies that she was not caught cheating. Thus in a generalized BB84 BC protocol, when Alice announces b to Bob, we say that Alice is attempting to unveil a bit b, but we only say that she has unveiled b if she passes Bob's test.
of the commitment phase, successfully unveil whatever bit she desires (given that Bob is honest). We denote these by $P_E$ and $P_U$ respectively. Note that these probabilities vary with the cheating strategy used. In this investigation, we shall only consider protocols wherein these are both equal to 1/2 for honest strategies.\footnote{In most discussions of bit commitment, it is assumed that neither Alice nor Bob has any information at the commitment phase about which bit will be more beneficial for Alice to unveil. However, one must relax this assumption in order to consider a game wherein Alice predicts which of two events will occur given some prior information on their relative probability. Our results can be generalized in a straightforward manner to apply to such a protocol. It suffices to replace Eq. (2.5) with $P_U = p_0 P_{U0} + p_1 P_{U1}$, where $p_0$ is the probability that Alice will wish to unveil bit $b$ after the commitment phase, and to generalize all subsequent expressions accordingly.}

The maxima of $P_E$ and $P_U$ for a given protocol, which we denote by $P_E^\text{max}$ and $P_U^\text{max}$, quantify the degree of concealment and the degree of bindingness that can be achieved in this protocol. If $P_E^\text{max}$ and $P_U^\text{max}$ are both strictly less than 1, the protocol is said to be \textit{partially binding} and \textit{partially concealing}.

The implementation of BC using a safe, discussed in the introduction, is binding against Alice, but is only concealing against Bob if he has limited ‘safe-cracking’ resources. More useful implementations of bit commitment instead rely for concealment on the assumption that Bob has limited computational resources. Obviously, one would prefer that the security of the protocol not depend on the resources of either party, but rather only on the laws of physics and the integrity of the party’s laboratories. A property of a protocol that has this feature is said to hold \textit{unconditionally}. All the properties of protocols referred to in this thesis are properties which hold unconditionally.

\subsection{2.2.3 Generalizations of the BB84 BC protocol}

A generalized BB84 BC protocol defines two sets of states $\{\psi^0_k\}_{k=1}^{n_0}$ and $\{\psi^1_k\}_{k=1}^{n_1}$ and corresponding probability distributions $\{p^0_k\}_{k=1}^{n_0}$ and $\{p^1_k\}_{k=1}^{n_1}$ (note that the values of $n_0$ and $n_1$ need not be the same). In order to commit to bit $b$, an honest Alice chooses a state from $\{\psi^b_k\}_{k=1}^{n_b}$ using the distribution $\{p^b_k\}_{k=1}^{n_b}$ and sends a system prepared in this state to Bob at the commitment phase. An honest Bob simply stores the system during
the holding phase. At the unveiling phase, an honest Alice announces \( b \) and \( k \) to Bob, and he measures the projector onto \( |\psi_k^b\rangle \). If Alice passes Bob's test, she has succeeded in unveiling the bit \( b \), and the result of the protocol is 'b'. Otherwise, she is caught cheating, and the result of the protocol is 'fail'.\(^3\)

To estimate Alice's commitment, Bob must estimate whether the system in his possession is described by \( \rho_0 = \sum_{k=1}^{n_0} p_k^0 |\psi_k^0\rangle \langle \psi_k^0| \), or \( \rho_1 = \sum_{k=1}^{n_1} p_k^1 |\psi_k^1\rangle \langle \psi_k^1| \). The problem of optimal state estimation has previously been studied in great detail [40][41], and in particular the optimal measurement for discriminating two density operators is known. Using the optimal measurement, the maximum probability of Bob correctly estimating Alice's commitment is

\[
P_E^{\text{max}} = \frac{1}{2} + \frac{1}{4} \text{Tr} |\rho_0 - \rho_1|.
\]

where \(|A| = \sqrt{A^\dagger A}\). It follows that as long as \( \rho_0 \) and \( \rho_1 \) are not orthogonal, \( P_E^{\text{max}} \) is strictly less than 1 and the protocol is partially concealing.

The complementary problem, of determining the maximum probability of Alice unveiling whatever bit she desires and the strategy which achieves this maximum, has remained open to date. Alice's most general strategy is of the following form. Prior to sending the system to Bob, she entangles it with a system she keeps in her possession. At the unveiling phase, she does one of two measurements on the system in her possession, depending on whether she is attempting to unveil a 0 or a 1. She chooses what integer \( k \) to announce to Bob based on the outcome of this measurement. It follows that in order to determine \( P_U^{\text{max}} \), we must optimize over the entangled state that Alice prepares, the two measurements she can perform and the announcement she makes to Bob given each possible outcome.

\(^3\)It should be noted that the honest strategy for Alice to commit \( b \) that we have described is equivalent with respect to concealment to the following strategy: Alice couples the system she sends to Bob with a system she keeps in her possession (of dimension \( n_0 \) or greater) such that the two are in the entangled state \( \sum_{k=1}^{n_0} \sqrt{p_k^0} |k\rangle \otimes |\psi_k^b\rangle \), where the \(|k\rangle \) form an orthonormal basis. At the unveiling phase, she measures the basis \(|k\rangle \) in order to determine what integer to announce to Bob.
It will be useful to introduce a few mathematical concepts and results before turning to the optimization problem.

2.3 Convex decompositions of a density operator

2.3.1 Definition and properties of convex decompositions

We begin by introducing a mathematical concept that will be critical for solving our problem. A convex decomposition \( \{(q_k, \sigma_k)\}_{k=1}^n \) of a density operator \( \rho \) is a set of probabilities, \( q_k \), and distinct density operators, \( \sigma_k \), such that

\[
\rho = \sum_{k=1}^n q_k \sigma_k.
\]

The \( \sigma_k \) will be referred to as the elements of the convex decomposition. We use the term 'convex' to distinguish this from a decomposition of a pure state into a sum of pure states, and from a decomposition of a density operator into general sums of operators, that is, sums of operators that are not necessarily positive. Nonetheless, we will throughout this chapter use the term decomposition as a shorthand.\(^4\)

Some terminology will be used in connection with convex decompositions. The elements that receive non-zero probability will be called the positively-weighted elements. A decomposition will be called extremal if its positively-weighted elements are all of rank 1 (i.e. if they are all pure states). A set of density operators will be called uncontractable if none of its members can be written as a convex decomposition of the others. A convex decomposition will be called uncontractable if its positively-weighted elements are uncontractable. Clearly, all extremal decompositions are uncontractable. Finally, a decomposition of \( \rho \) is trivial if its only positively-weighted element is \( \rho \).

Another concept that will be useful in the present investigation is a relation that holds

\(^4\)Note that previous authors have used the term \( \rho \)-ensemble to refer to a convex decomposition of \( \rho \).
between sets of density operators, and which we shall refer to as *composable coincidence*.

Two sets of density operators \( \{ \sigma_k^0 \} \) and \( \{ \sigma_k^1 \} \) will be called compositely coincident if there exist probability distributions \( \{ q_k^0 \} \) and \( \{ q_k^1 \} \) such that

\[
\sum_k q_k^0 \sigma_k^0 = \sum_k q_k^1 \sigma_k^1.
\]

In other words, \( \{ \sigma_k^0 \} \) and \( \{ \sigma_k^1 \} \) are compositely coincident if there exists a density operator which has a convex decomposition in terms of the \( \sigma_k^0 \)'s and a convex decomposition in terms of the \( \sigma_k^1 \)'s.

It will also be useful to set forth a few well-known facts about convex decompositions [42]. A necessary and sufficient condition for a density operator \( \sigma \) to appear in some convex decomposition of \( \rho \) is for the eigenvectors of \( \sigma \) to be confined to the support of \( \rho \). The cardinality of an extremal decomposition of \( \rho \) must be greater than or equal to the rank of \( \rho \). Finally, there sometimes exists a prescription for obtaining the probability with which a particular element appears in a convex decomposition of a density operator. In convex decompositions of \( \rho \) containing *orthogonal* elements, the probability associated with an element \( \sigma \) is fixed by \( \rho \) and \( \sigma \) - it is simply \( \text{Tr}(\sigma \rho)/\text{Tr}(\sigma^2) \). However, for a general set of non-orthogonal elements \( \{ \sigma_k \} \) that form a convex decomposition of \( \rho \), the probabilities need not be unique: the same set of density operators \( \{ \sigma_k \} \) may appear in different convex decompositions of \( \rho \). For instance, the completely mixed state in a 2d Hilbert space, \( I/2 \), has an indenumerably infinite number of convex decompositions with elements \( \{ |0\rangle \langle 0|, |1\rangle \langle 1|, |+\rangle \langle +|, |-\rangle \langle -| \} \), since these yield a decomposition for every probability distribution of the form \( \left( \frac{1}{2} \lambda, \frac{1}{2} \lambda, \frac{1}{2} (1 - \lambda), \frac{1}{2} (1 - \lambda) \right) \) where \( \lambda \) is between 0 and 1. Nonetheless, a special case wherein the probabilities are unique is if the convex decomposition is extremal and of cardinality equal to the rank of \( \rho \). In this case, a simple formula for the probability of a given element can be given. If \( \{ (q_k, |\xi_k\rangle \langle \xi_k|) \} \) is such a decomposition, then the non-zero probabilities are given by Jaynes' rule [43].
where $\rho^{-1}$ is the inverse of the restriction of $\rho$ to its support (in other words, $\rho^{-1}$ is obtained from $\rho$ by inverting the non-zero eigenvalues in the spectral resolution of $\rho$).

### 2.3.2 The connection between convex decompositions and POVMs

The most general measurement on a system in quantum mechanics is associated with a positive operator valued measure (POVM) [44]. A POVM is a set of positive operators that sum to the identity operator, that is, a set $\{E_k\}$ such that for every $k$, $\langle \phi | E_k | \phi \rangle \geq 0$ for all $|\phi\rangle \in \mathcal{H}$, and $\sum_k E_k = I$. A measurement associated with the POVM $\{E_k\}$ has as many outcomes as there are elements in the POVM. If such a measurement is made on a system in the state $\rho$, the probability of outcome $k$ is $\text{Tr}(\rho E_k)$. Neumark's theorem [45] shows that every POVM on a system can be implemented by coupling to an ancilla system and performing projective measurements on the ancilla. As it turns out, there is a close mathematical connection between convex decompositions of $\rho$ and POVMs, as was demonstrated by Hughston, Jozsa and Wootters [42].

**Lemma** There is a one-to-one map between the convex decompositions of $\rho$ and the POVMs over the support of $\rho$. Specifically, the POVM $\{E_k\}_{k=1}^n$ is associated with the decomposition $\{(q_k, \sigma_k)\}_{k=1}^n$ defined by

$$q_k = \frac{1}{\langle \xi_k | \rho^{-1} | \xi_k \rangle},$$

where $\rho^{-1}$ is the inverse of the restriction of $\rho$ to its support (in other words, $\rho^{-1}$ is obtained from $\rho$ by inverting the non-zero eigenvalues in the spectral resolution of $\rho$).

**Proof.** It is trivial to see that $\{(q_k, \sigma_k)\}_{k=1}^n$ is a decomposition of $\rho$ by summing the above equation over $k$ and using the fact that $\sum_k E_k = I$. That any decomposition of $\rho$ is associated with some POVM follows from the fact that $\sqrt{\rho}$ is invertible on the support of $\rho$. Specifically, if this inverse is denoted by $\rho^{-1/2}$ then the resolution $\{(q_k, \sigma_k)\}_{k=1}^n$ is...
associated with the POVM \( \{ E_k \}_{k=1}^n \) defined by \( E_k = q_k \rho^{-1/2} \sigma_k \rho^{-1/2} \).

We will also say that the POVM \( \{ E_k \}_{k=1}^n \) generates the convex decomposition \( \{(q_k, \sigma_k)\}_{k=1}^n \).

Note that we do not treat the technicalities associated with decompositions of infinite cardinality here, however a discussion of these can be found in Cassinelli et al. [46].

### 2.3.3 The significance of convex decompositions for coherent attacks

Suppose Alice and Bob share an entangled state for which \( \rho \) is the reduced density operator on Bob’s system. Prior to any measurements, the best Alice can do in predicting the outcomes of Bob’s measurements is to use the density operator \( \rho \) in the Born rule. However, by virtue of the correlations between her system and Bob’s, if she performs a measurement and takes note of the outcome, her ability to predict the outcomes of Bob’s measurements will increase. Since all of the information that is relevant to Alice predicting the outcomes of Bob’s measurements is encoded in a density operator, it follows that when she learns the outcome of her measurement, she should update the density operator with which she describes Bob’s system. Suppose that the \( k \)th outcome occurs with relative frequency \( q_k \), and leads Alice to update the density operator with which she describes Bob’s system to \( \sigma_k \). We say that the statistics of possible updates of Alice’s description of Bob’s system are given by \( \{(q_k, \sigma_k)\} \), that is, a set of probabilities and density operators.

As it turns out, the possibilities for these statistics are given by the convex decompositions of \( \rho \). Specifically, we have:

**HJW Theorem** For every measurement Alice can do, the statistics of possible updates of her description is given by some convex decomposition of \( \rho \), and for every convex decomposition of \( \rho \), there exists some measurement for which the statistics of possible updates is given by that decomposition.
This was first demonstrated for extremal convex decompositions by Hughston, Jozsa and Wootters [42], and it is straightforward to generalize the proof to arbitrary convex decompositions. Since this theorem is the key to coherent attacks, we present the proof here.

**Proof.** Suppose Alice and Bob share a state $|\psi\rangle$ that is a purification of a density operator $\rho$ defined on Bob's system (a purification of $\rho$ is any normalized vector $|\Phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ with $\text{Tr}_A (|\Phi\rangle \langle \Phi|) = \rho$). If the non-zero eigenvalues of $\rho$ are denoted by $\lambda_j$, and $\{e_j\}$ is a set of normalized eigenvectors associated with these eigenvalues, then $|\psi\rangle$ can always be written as

$$|\psi\rangle = \sum_j \sqrt{\lambda_j} |f_j\rangle \otimes |e_j\rangle,$$

where $\{f_j\}$ is a set of orthonormal vectors for Alice's system. Note that $\{e_j\}$ and $\{f_j\}$ need not span $\mathcal{H}_A$ or $\mathcal{H}_B$ respectively, but the subspaces which they do span are necessarily of equal dimensionality. This way of writing $|\psi\rangle$ is known as the bi-orthogonal or Schmidt decomposition.

We begin by specifying the measurement that Alice must do on her system in order to have her statistics of possible updates given by the convex decomposition $\{(q_k, \sigma_k)\}$ of $\rho$. If the POVM on Bob's system that generates this decomposition is denoted by $\{E_k\}$, so that

$$q_k \sigma_k = \sqrt{\rho} E_k \sqrt{\rho},$$

and $U$ is the unitary map that satisfies

$$|f_j\rangle = U |e_j\rangle,$$

then the required measurement on Alice's system is the one associated with the POVM $\{U E_k U^\dagger\}_{k=1}^n$. The proof is as follows.
The entangled state Alice and Bob share can be written in terms of $U$ as

$$|\psi\rangle = \sum_{j} \sqrt{\lambda_j} U |e_j\rangle \otimes |e_j\rangle.$$ 

Upon measuring the POVM $\{U E_k U^\dagger\}$ on her system and obtaining outcome $k$, the projection postulate for POVMs dictates that Alice should describe Bob's system by the unnormalized state

$$\text{Tr}_A \left( \sqrt{U E_k U^\dagger} |\psi\rangle \langle \psi| \sqrt{U E_k U^\dagger} \right)$$

$$= \left( \sum_{j} \sqrt{\lambda_j} |e_j\rangle \langle e_j| \right) E_k \left( \sum_{j'} \sqrt{\lambda_{j'}} |e_{j'}\rangle \langle e_{j'}| \right)$$

$$= \sqrt{\rho E_k \sqrt{\rho}}$$

$$= q_k \sigma_k.$$ 

So after this measurement, with probability $q_k$ Alice updates the density operator with which she describes Bob's system to $\sigma_k$.

It is also easy to show that the statistics of possible updates are given by some convex decomposition of $\rho$ for every measurement Alice can do. This follows from the fact that every measurement on Alice's system can be described by a POVM of the form $\{U E_k U^\dagger\}$ for some choice of $\{E_k\}$ given a particular $U$. \(\square\)

When Alice entangles the system she submits to Bob with a system she keeps in her possession in such a way that Bob's reduced density operator is $\rho$, we shall say that Alice submits $\rho$ to Bob. When Alice performs a measurement that leads to her statistics of possible updates being given by the convex decomposition $\{(q_k, \sigma_k)\}$ of $\rho$, we shall say that Alice realizes this decomposition on Bob's system.
2.4 The nature of the optimization problem

In section 2.2.4, we formulated the problem of determining the optimal cheat strategy for Alice as a variational problem over the entangled state that she initially prepares and the measurements she performs on her half of the system. However, from the results of section 2.3.3 it is clear that in determining Alice's probability of unveiling the bit of her choosing, all that is important about the entangled state she prepares is the reduced density operator \( \rho \) she submits to Bob, and all that is important about the measurement she performs is the convex decomposition of \( \rho \) that she thereby realizes. It suffices therefore to vary over \( \rho \) and its convex decompositions.

We begin by showing that if Alice is attempting to unveil a bit \( b \) then it suffices for her to realize a convex decomposition with a number of elements less than or equal to \( n_b \). The proof is as follows. Suppose Alice realizes a convex decomposition \( \{ (\bar{q}_j, \bar{\sigma}_j) \}_{j=1}^{n'} \) with a number of elements \( n' \) that is greater than \( n_b \). She still must announce to Bob an index between 1 and \( n_b \), so that the elements of this decomposition must be grouped into \( n_b \) sets, where elements in the \( k \)th set, \( S_k \), correspond to announcing the index \( k \) to Bob. When Alice announces index \( k \), Bob will measure the projector \( |\psi_k^b\rangle \langle \psi_k^b| \) and obtain a positive result with probability \( \sum_{j \in S_k} \bar{q}_j \langle \psi_k^b | \bar{\sigma}_j | \psi_k^b \rangle \). However, there is always an \( n_b \)-element convex decomposition that yields the same probability of a positive result as the one considered here; specifically, the decomposition \( \{ (q_k, \sigma_k) \}_{k=1}^{n_b} \) with \( q_k \sigma_k = \sum_{j \in S_k} \bar{q}_j \bar{\sigma}_j \).

It follows that the probability of Alice succeeding at unveiling the bit \( b \) given that she submits \( \rho \) and realizes a convex decomposition \( \{ (q_k, \sigma_k) \}_{k=1}^{n_b} \) of \( \rho \) is

\[
P_{Ub} = \sum_{k=1}^{n_b} q_k \langle \psi_k^b | \sigma_k | \psi_k^b \rangle. \tag{2.4}
\]

Thus, if Alice submits \( \rho \) and realizes the convex decompositions \( \{ (q_k^0, \sigma_k^0) \}_{k=1}^{n_0} \) and \( \{ (q_k^1, \sigma_k^1) \}_{k=1}^{n_1} \) to unveil bit values of 0 and 1 respectively, then if she is equally likely to wish to unveil 0 as 1 (as we are assuming in this investigation), her probability of unveiling the bit of
The task is to maximize $P_U$ with respect to variations in $\rho$. \{$(q^0_k, \sigma^0_k)\}_{k=1}^{n_0}$ and \{$(q^1_k, \sigma^1_k)\}_{k=1}^{n_0}$ subject to the constraint that $\rho = \sum_{k=1}^{n_0} q^0_k \sigma^0_k = \sum_{k=1}^{n_1} q^1_k \sigma^1_k$.

It is useful to divide this optimization problem into two steps. In the first step one determines, for an arbitrary but fixed $\rho$, the $n_b$-element convex decomposition of $\rho$ that maximizes the probability $P_{Ub}$ of Alice unveiling the bit $b$. Given this solution, the probability $P_U$ of Alice unveiling the bit of her choosing can be expressed entirely in terms of the submitted $\rho$. In the second step one determines the $\rho$ that maximizes $P_U$.

### 2.5 Results for general protocols

#### 2.5.1 The connection to state estimation

We will show that the problem of optimizing the convex decomposition for an arbitrary but fixed density operator has an intimate connection to the problem of optimal state estimation. As discussed in section 2.3.2, for every convex decomposition \{$(q_k, \sigma_k)$\}$_k$ there exists a POVM \{${E_k}$\}. defined over the support of $\rho$, that generates this decomposition as in Eq. (2.3). Thus, Eq. (2.4) can be written as

$$P_{Ub} = \sum_{k=1}^{n_b} \langle \psi^b_k | \sqrt{\rho} E_k \sqrt{\rho} | \psi^b_k \rangle.$$
A set of normalized states \( \{ \chi_k^b \} \) and probabilities \( \{ w_k^b \} \) can be defined in terms of \( \rho \) and \( \{ \psi_k^b \} \) as follows:

\[
| \chi_k^b \rangle = \frac{\sqrt{\rho} | \psi_k^b \rangle}{\sqrt{\langle \psi_k^b | \rho | \psi_k^b \rangle}},
\]

\[
w_k^b = \frac{\langle \psi_k^b | \rho | \psi_k^b \rangle}{\sum_k \langle \psi_k^b | \rho | \psi_k^b \rangle}.
\]

In terms of these, \( P_{U_b} \) has the form

\[
P_{U_b} = C \sum_{k=1}^{n_b} w_k^b \langle \chi_k^b | E_k | \chi_k^b \rangle,
\]

where \( C = \sum_k \langle \psi_k^b | \rho | \psi_k^b \rangle \).

We now recall [40] the problem of estimating the state of a system that is known to have been prepared in one of \( n_b \) states \( \{ \chi_k^b \} \) with prior probabilities \( \{ w_k^b \} \). The most general type of measurement is a POVM measurement, and it suffices to consider POVMs that have \( n_b \) elements (this is established by an argument exactly analogous to the one provided above for the sufficiency of \( n_b \)-element decompositions in optimizing over coherent attacks). For a measurement of the POVM \( \{ E_k \} \), the probability of estimating correctly is \( \sum_{k=1}^{n} w_k^b \langle \chi_k^b | E_k | \chi_k^b \rangle \).

The connection between our problem and the state estimation problem is now clear. If \( \{ \chi_k^b \} \) and \( \{ w_k^b \} \) are defined by Eqs. (2.6) and (2.7), and \( \{ E_k \} \) is defined by (2.3), then the following relation holds. The probability of unveiling a bit \( b \), associated with a set of states \( \{ \psi_k^b \} \), when Bob's reduced density operator is \( \rho \), given that Alice's strategy consists of realizing an \( n_b \)-element convex decomposition \( \{ (q_k, \sigma_k) \} \) of \( \rho \), is a constant multiple of the probability of correctly estimating the state of a system, known to be prepared in one of \( n_b \) states \( \{ \chi_k^b \} \) with prior probabilities \( \{ w_k^b \} \), given a measurement of the POVM \( \{ E_k \} \).

So, if one has the solution to the problem of finding the POVM that maximizes the
probability of correctly estimating the state of a system from among a set of pure states. then one also has the solution to the problem of finding the convex decomposition of \( \rho \) that Alice should realize to maximize her probability of passing Bob's test. There is a \textit{duality} between these two information theoretic tasks.

This result is very useful since it connects a task about which very little is known to one about which a great deal is known. In particular, one is able to infer some general features of the optimal cheat strategy by appealing to some well-known theorems on state estimation.

One such feature is that if the \( \{ \psi^k \} \) are linearly independent, and the support of \( \rho \) is the span of the \( \{ \psi^k \} \), then the optimal convex decomposition of \( \rho \) is extremal. The proof is as follows. If the \( \{ \psi^k \} \) are linearly independent and span the support of \( \rho \), then the \( \{ \chi^k \} \) are linearly independent. It is well known that in estimating a state drawn from a set of linearly independent states, the optimal POVM has elements of rank 1 [40]. The convex decomposition that is generated by such a POVM has elements that are pure states, \textit{i.e.}, it is extremal.

2.5.2 The support of the optimal density operator

We now turn to the problem of determining the optimal density operator for Alice to submit to Bob. We begin by showing that although Alice could cheat by submitting a system with more degrees of freedom than the honest protocol specifies, she gains no advantage by doing so. In other words, the optimal \( \rho \) has a support that is equal to or a subspace of the span of \( \{ \psi^k \}_{k=1}^{n_0} \cup \{ \psi^1 \}_{k=1}^{n_1} \). We establish this by showing that for any \( \rho^* \) that has support strictly greater than this span, there is a \( \rho \) that has support that is equal to or a subspace of this span and that yields a greater value of \( P_U \). Suppose the optimal convex decomposition of \( \rho^* \) for unveiling bit \( b \) is denoted \( \{ (q^k_b, \sigma^k_b) \}_{k=1}^{n_b} \). The
maximum probability of Alice unveiling the bit of her choosing using $\rho^*$ is then

$$P_{U_{\text{max}}}^\text{max} (\rho^*) = \frac{1}{2} \sum_{b=0}^{1} \sum_{k=1}^{n_b} \langle \psi_k^b | q_k^b \sigma_k^b | \psi_k^b \rangle.$$

However, if Alice submits the density operator

$$\rho = G \rho^* G / \text{Tr} (\rho^* G),$$

where $G$ is the projector onto the span of $\{ \psi_k^0 \}_{k=1}^{n_0} \cup \{ \psi_k^1 \}_{k=1}^{n_1}$, and realizes the convex decomposition $\{ (q_k^b, \sigma_k^b) \}_{k=1}^{n_b}$ defined by $q_k^b \sigma_k^b = G q_k^b \sigma_k^b G / \text{Tr} (\rho^* G)$, then her probability of unveiling whatever bit she desires is

$$P_U (\rho) = P_{U_{\text{max}}}^\text{max} (\rho^*) / \text{Tr} (\rho^* G).$$

Since $\text{Tr} (\rho^* G) < 1$, it follows that $P_U (\rho) > P_{U_{\text{max}}}^\text{max} (\rho^*)$.

2.5.3 Conditions for unveiling with certainty

Finally, we consider the question of whether, for a particular protocol. Alice can unveil the bit of her choosing with certainty. The necessary and sufficient condition for there to be a strategy that makes $P_{U_b} = 1$ for a given $b$, is that $\rho$ is decomposed by the set of states $\{ \psi_k^b \}_{k=1}^{n_b}$, that is, there must exist a probability distribution $\{ q_k^b \}_{k=1}^{n_b}$ such that $\{ (q_k^b, | \psi_k^b \rangle \langle \psi_k^b |) \}_{k=1}^{n_b}$ forms a convex decomposition of $\rho$. The necessary and sufficient condition for there to be a strategy that makes $P_U = 1$ is that there exists a $\rho$ that is decomposed by both $\{ \psi_k^0 \}_{k=1}^{n_0}$ and $\{ \psi_k^1 \}_{k=1}^{n_1}$. In the terminology of section 2.3.1, $\{ \psi_k^0 \}_{k=1}^{n_0}$ and $\{ \psi_k^1 \}_{k=1}^{n_1}$ must be compositively coincident.

The results described in this section constitute all that we shall say about the optimal cheat strategy for an arbitrary protocol. Hereafter, we shall restrict ourselves to the special case of sets $\{ \psi_k^0 \}_{k=1}^{n_0}$ and $\{ \psi_k^1 \}_{k=1}^{n_1}$ whose union span at most a two dimensional
Hilbert space, that is, protocols that can be implemented using a single qubit.

2.6 Results for qubit protocols

2.6.1 The Bloch ball representation

Our optimization problem is greatly simplified in the case of a 2D Hilbert space since there is a one-to-one mapping between the set of all density operators in such a space and the set of all points within the unit ball of $\mathbb{R}^3$. For clarity, we begin by reminding the reader about the details of this mapping.

If one defines an inner product between operators $A$ and $B$ by $\text{Tr} (A^\dagger B)$, the set of operators over a Hilbert space forms an inner product space. In a 2d Hilbert space, a particularly convenient orthogonal basis for the set of operators is the set of Pauli operators $\{\sigma_x, \sigma_y, \sigma_z, I\}$, with matrix representations in the $\{|0\rangle, |1\rangle\}$ basis of

\[
\begin{align*}
\sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \\
\sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{align*}
\]

Any operator $A$ can therefore be written as $A = \frac{1}{2} (a_0 I + \vec{a} \cdot \vec{\sigma})$ where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ and $\vec{a} = (a_x, a_y, a_z)$, with $a_0, a_x, a_y, a_z \in \mathbb{C}$. In particular, for a density operator $\rho$, the constraints of unit trace ($\text{Tr}(\rho) = 1$) and positivity ($\text{det}(\rho) \geq 0$) imply that

\[
\rho = \frac{1}{2} (I + \vec{r} \cdot \vec{\sigma}),
\]

where $\vec{r} \in \mathbb{R}^3$ and $|\vec{r}| \leq 1$.

Thus we see that every density operator is represented by a vector $\vec{r}$ within the unit ball.
of \( \mathbb{R}^3 \), which we shall refer to as the Bloch ball.\(^5\)

Density operators describing pure states are characterized by a vanishing determinant, \( \det(\rho) = 0 \), which corresponds to a vector of unit length, \(|\vec{r}| = 1\) that we shall sometimes denote by \( \vec{r} \). Thus, pure states are represented by the points on the surface of the ball. The completely mixed state, \( \rho = \frac{1}{2} I \), is represented by \( \vec{r} = \vec{0} \), which is the point at the centre of the ball. If two density operators \( \rho_1 \) and \( \rho_2 \) are represented by vectors \( \vec{r}_1 \) and \( \vec{r}_2 \), the inner product between \( \rho_1 \) and \( \rho_2 \) is given by \( \text{Tr}(\rho_1 \rho_2) = \frac{1}{2} (1 + \vec{r}_1 \cdot \vec{r}_2) \). It follows that orthogonal states are represented by antipodal points, since \( \text{Tr}(\rho_1 \rho_2) = 0 \) implies \( \vec{r}_1 \cdot \vec{r}_2 = -1 \).

We are now in a position to obtain a representation on the Bloch ball of all the density operators that can be formed by convex combination of a particular set of elements \( \{\sigma_k\}_{k=1}^n \), that is, all the \( \rho \) that have the form

\[
\rho = \sum_{k=1}^n q_k \sigma_k
\]

for some probability distribution \( \{q_k\}_{k=1}^n \). Since the set of density operators that can be formed by an arbitrary set of elements \( \{\sigma_k\}_{k=1}^n \) is the same as the set that can be formed by an uncontractable set of elements from which all the states in \( \{\sigma_k\}_{k=1}^n \) can be built up by convex combination, it suffices to consider only uncontractable sets of elements.

Denoting the Bloch vectors associated with \( \rho \) and \( \sigma_k \) by \( \vec{r} \) and \( \vec{s}_k \) respectively, we find the relevant set to be given by

\[
\vec{r} = \sum_{k=1}^n q_k \vec{s}_k, \text{ where } 0 \leq q_k \leq 1. \sum_{k=1}^n q_k = 1.
\]

To understand what this manifold of points looks like, consider the simplest case of \( n = 2 \).

\(^5\)The surface of the ball is usually referred to as the Bloch sphere or the Riemann sphere in the context of spins, and the Poincare sphere in the context of photon polarization.
The above equation can then be written as

\[ \vec{r} = \vec{s}_1 + \lambda (\vec{s}_2 - \vec{s}_1), \text{ where } 0 \leq \lambda \leq 1. \]

This is simply the parametric equation for a segment of a straight line extending between \( \vec{s}_1 \) and \( \vec{s}_2 \). Similarly, in the case of \( n = 3 \), we have

\[ \vec{r} = \vec{s}_1 + \lambda (\vec{s}_2 - \vec{s}_1) + \xi (\vec{s}_3 - \vec{s}_2), \]

where \( 0 \leq \lambda \leq 1 \) and \( 0 \leq \xi \leq \lambda \).

Since \( \sigma_1, \sigma_2 \) and \( \sigma_3 \) were assumed to form an uncontractable set of elements, \( \vec{s}_1, \vec{s}_2 \) and \( \vec{s}_3 \) cannot lie on a line, and therefore define the vertices of a triangle. The above equation is the parametric equation for the surface of points inside this triangle. For \( n = 4 \), we have

\[ \vec{r} = \vec{s}_1 + \lambda (\vec{s}_2 - \vec{s}_1) + \xi (\vec{s}_3 - \vec{s}_2) + \zeta (\vec{s}_4 - \vec{s}_3), \]

where \( 0 \leq \lambda \leq 1, 0 \leq \xi \leq \lambda \) and \( 0 \leq \zeta \leq \xi \).

Again, since \( \sigma_1, \sigma_2, \sigma_3 \) and \( \sigma_4 \) were assumed to form an uncontractable set of elements, none of \( \vec{s}_1, \vec{s}_2, \vec{s}_3 \) or \( \vec{s}_4 \) can lie along the line segment defined by any other two, nor inside the surface of the triangle defined by any other three, and thus these vectors define the vertices of either a convex quadrilateral or a tetrahedron. The above equation is the parametric equation for the surface of points inside this quadrilateral, or the volume of points inside this tetrahedron. Similarly, for greater than 4 uncontractable elements, we obtain the parametric equation for the points inside an \( n \)-vertex convex polygon or convex polyhedron. All told, in the case of a set of \( n \) uncontractable elements, the set of density operators that can be composed from these will be represented by the region inside an \( n \)-vertex convex polytope. A few different sets of states and the density operators that can be composed from them are depicted in Fig. 2.1.
Figure 2.1: A depiction of three sets of states containing 2, 3 and 4 elements respectively. The points in the Bloch ball representing these states are indicated by small black spheres. The manifolds inside the line segment, triangle and tetrahedron that are defined by each set of points represent all the density operators that can be composed with each set of states.

It is now easy to see the solution to a complementary problem, namely, how to obtain a representation on the Bloch ball of all the uncontractable convex decompositions of a particular density operator $\rho$. If $\rho$ is represented by the point $\bar{r}$, then every $n$-element uncontractable convex decomposition of $\rho$ is represented by an $n$-vertex convex polytope which contains $\bar{r}$. For instance, every 2-element uncontractable convex decomposition of $\rho$ is represented by a line segment that contains $\bar{r}$; every 3-element uncontractable convex decomposition of $\rho$ is represented by a triangle that contains $\bar{r}$ and so forth. In Fig. 2.2, we illustrate a few of the convex decompositions of a fixed density operator. Of particular interest to us in the present context are extremal convex decompositions of a density operator $\rho$ (which are always uncontractable). Since pure states are associated with unit Bloch vectors, the convex polytopes associated with such decompositions have their vertices on the surface of the Bloch ball. Fig. 2.2 provides an example of this distinction.
Figure 2.2: An illustration of three convex decompositions of a fixed density operator, two of which are 2-element decompositions, and one of which is a 3-element decomposition. The point in the Bloch ball representing the density operator is indicated with a large black sphere. Each convex decomposition is represented by a polytope containing the point representing the density operator, the vertices of which represent the elements of the decomposition. These are indicated in grey. The longer of the two line segments, which has its vertices on the surface of the Bloch ball, is an example of an extremal convex decomposition.

Figure 2.3: A depiction of a fixed density operator and two sets of states; the bottom set decomposes the density operator, while the upper set does not.
2.6.2 The conditions under which Alice can unveil the bit of her choosing with certainty

In section 2.5.3 it was pointed out that a strategy with $P_{ub} = 1$ exists if and only if $\rho$ is decomposed by the states $\{\psi^b_k\}_{k=1}^n$. The Bloch ball representation gives a simple way of testing whether this condition is satisfied for protocols restricted to a 2D Hilbert space. It suffices to plot the convex polytope whose vertices are the points representing the $\{\psi^b_k\}_{k=1}^n$ and to determine whether the point representing $\rho$ is contained in this polytope or not. If it is, then Alice can unveil bit $b$ with certainty. If it is not, then she cannot. An example of the two possibilities is provided in Fig. 2.3.

More importantly, we can now answer the question of whether there exists a strategy for Alice with $P_U = 1$ for protocols restricted to a 2D Hilbert space. As pointed out in section 2.5.3 this only occurs if the two sets of states are compositively coincident. It is clear now how to verify whether this is the case or not. Simply plot the convex polytopes associated with both sets of states, and determine whether they intersect one another or not. If they do, then any point inside the region of intersection corresponds to a density operator that is decomposed by both sets and consequently lets Alice unveil the bit of her choosing with probability 1. If they do not, then this probability is strictly less than 1.

The convex polytopes associated with the sets of states used in the BB84 BC protocol are depicted in Fig. 2.4. Since these cross at the origin, it follows that if Alice submits to Bob the completely mixed state, she can achieve $P_U = 1$. So we simply have a restatement of the fact that if Alice initially prepares a maximally entangled state, such as the EPR state, and submits half to Bob, then she can achieve $P_U = 1$. The protocols we shall consider hereafter are associated with non-intersecting convex polytopes. See Figs. 2.6-2.10 for examples.
2.6.3 Optimizing over the convex decompositions of an arbitrary but fixed density operator

We now turn to the problem of determining the optimal EPR cheating strategy for a qubit protocol. We do not solve this problem completely; rather, we solve it under the further restriction that each set contains only linearly independent states. In the present 2D context, linear independence implies that each set can have no more than two elements.

As discussed in section 2.4, it is useful to split the problem into two parts involving optimization over convex decompositions of an arbitrary but fixed density operator, followed by optimization over density operators. We address these two parts of the problem in this section and the next section respectively.

We begin with the problem of maximizing the probability, $P_{Ub}$, that Alice can unveil the bit $b$ given that she submitted a density operator $\rho$. This maximum must be found with respect to variations in the convex decomposition of $\rho$ that she realizes. The optimal decomposition will depend on $\rho$ and the states in the set $\{\psi_k^b\}_{k=1}^{n_b}$. In order to simplify the notation in this section, we drop the index $b$ from $|\psi_k^b\rangle$ and $n_b$. We also assume that
\( \rho \) is impure, since otherwise there is no optimization problem to be solved.

**A set containing one element (\( n = 1 \))**

In this case, Bob's test is fixed (he always measures the projector onto some fixed state \( |\psi_1\rangle \)), so the probability of passing this test depends only on \( \rho \) and not on the convex decomposition of \( \rho \) that Alice realizes. Thus, there is no optimization over decompositions to be performed in this case.

**A set containing two elements (\( n = 2 \))**

Let the Bloch vectors associated with \( |\psi_k\rangle \) and \( \rho \) be denoted by \( \hat{a}_k \) and \( \bar{r} \) respectively, and let those associated with the elements, \( \sigma_k \), of the two-element convex decomposition \( \{(q_k, \sigma_k)\}_{k=1}^2 \) that Alice realizes be denoted by \( \bar{s}_k \). In terms of these, Alice's probability of passing Bob's test, specified by Eq. (2.4), has the following form

\[
P_{Ub} = \frac{1}{2} \left( 1 + \sum_{k=1}^2 q_k (\hat{a}_k \cdot \bar{s}_k) \right). 
\]  

We must maximize this subject to the constraint that \( \bar{r} = \sum_k q_k \bar{s}_k \).

We find that the optimal convex decomposition of \( \bar{r} \) is given by

\[
\begin{align*}
\bar{s}_1^{\text{opt}} &= \bar{r} + L_+ (\bar{r}) \hat{d}, \\
\bar{s}_2^{\text{opt}} &= \bar{r} + L_- (\bar{r}) \hat{d}.
\end{align*}
\]  

and

\[
q_k^{\text{opt}} = \frac{1 - |\bar{r}|^2}{2 |1 - \bar{r} \cdot \bar{s}_k^{\text{opt}}|} 
\]  

where

\[
L_\pm (\bar{r}) = -\bar{r} \cdot \hat{d} \pm \sqrt{1 - |\bar{r}|^2 + (\bar{r} \cdot \hat{d})^2}.
\]
Figure 2.5: An illustration of the optimal convex decomposition for Alice to realize when she has submitted to Bob a fixed density operator (indicated by the large black sphere) and is attempting to convince him that he has one of two states (indicated by the small black spheres). This is represented by the chord (indicated in grey) that is parallel to the chord defined by the two states. After Alice realizes this decomposition (by making a measurement on the system that is entangled with Bob's), she updates her description of Bob's system to whichever of the elements it happened to be collapsed to (indicated by the grey spheres). When it comes time for Alice to announce to Bob which of the two states he should test for to verify her honesty, she announces the state which has the smallest angular separation from the element of the decomposition onto which she has collapsed his system.

and

$$\hat{d} = \frac{\hat{a}_1 - \hat{a}_2}{|\hat{a}_1 - \hat{a}_2|}. \tag{2.12}$$

Note that $|\hat{s}_1^{\text{pt}}| = |\hat{s}_2^{\text{pt}}| = 1$, which means that this is an extremal convex decomposition. The proof of optimality is presented in Appendix A.

This solution has a very simple geometrical description. It is the convex decomposition that is represented by the chord (i.e., line segment whose endpoints lie on the surface of the ball) that contains $\bar{r}$ and that is parallel to the chord defined by $\hat{a}_1, \hat{a}_2$. An example is presented in Fig. 2.5.

The corresponding probability of passing Bob's test is simply

$$P_{\text{Ub}}^{\text{max}} = \frac{1}{2} \left( 1 + (\bar{r} + L_+ (\bar{r} \hat{d}) \cdot \hat{a}_1) \right).$$
In Hilbert space language,
\[ P_{UB}^{\text{max}} = \frac{1}{2} \frac{(\langle \psi_1 | \rho | \psi_1 \rangle + \langle \psi_2 | \rho | \psi_2 \rangle)}{\sqrt{2(1 - \text{Tr}(\rho^2)) (\langle \psi_1 | \psi_2 \rangle)^2 + (\langle \psi_1 | \rho | \psi_1 \rangle - \langle \psi_2 | \rho | \psi_2 \rangle)^2}}. \]

### 2.6.4 Optimizing over density operators

We now consider the problem of determining the optimal density operator \( \rho \) for Alice to submit to Bob in order to maximize her probability of unveiling the bit of her choosing. The solution will depend on the values of \( n_0 \) and \( n_1 \). Given that we are assuming that the states in the sets \( \{ \psi_k^0 \}_{k=1}^{n_0} \) and \( \{ \psi_k^1 \}_{k=1}^{n_1} \) are linearly independent, there are only three possibilities to address: both sets contain two elements; one set contains two elements and the other contains one element; both sets contain one element. We shall consider each of these in turn.

**Both sets contain two elements** \((n_0 = n_1 = 2)\)

Denote the Bloch vector associated with the state \( | \psi_k^b \rangle \) by \( \hat{\alpha}_k^b \). The result of the previous section indicates that whatever the optimal \( \vec{r} \) is, the optimal convex decomposition for unveiling bit \( b \) is represented by the chord passing through \( \vec{r} \) parallel to the chord defined by \( \hat{\alpha}_1^b, \hat{\alpha}_2^b \). We therefore have that Alice's probability of unveiling the bit of her choosing given an arbitrary \( \vec{r} \) and given that when she attempts to unveil the bit \( b \) she realizes the convex decomposition of \( \vec{r} \) that is optimal for doing so, is simply

\[ P_U = \sum_{b=0}^{1} \frac{1}{4} \left( 1 + \left( \vec{r} + L_{b+}(\vec{r}) \hat{d}_b \right) \cdot \hat{a}_1^b \right), \tag{2.13} \]

where \( \hat{d}_b = \frac{\hat{a}_1^b - \hat{a}_2^b}{|\hat{a}_1^b - \hat{a}_2^b|} \) and

\[ L_{b+}(\vec{r}) = -\vec{r} \cdot \hat{d}_b + \sqrt{1 - |\vec{r}|^2 + (\vec{r} \cdot \hat{d}_b)^2}. \]
It will be convenient to adopt the convention that the states in the protocol are indexed in such a way that $\langle \psi_{k}^{0} | \psi_{1}^{0} \rangle = \max_{k, k'} \langle \psi_{k}^{0} | \psi_{k'}^{0} \rangle$. In terms of the Bloch ball, the convention states that if one draws the chords defined by $\hat{a}_{1}^{0}, \hat{a}_{2}^{0}$ and $\hat{a}_{1}, \hat{a}_{2}$, the endpoints $\hat{a}_{1}^{0}$ and $\hat{a}_{1}$ have the smallest separation.

We consider two cases.

Case 1: The chords defined by $\hat{a}_{1}^{0}, \hat{a}_{2}^{0}$ and $\hat{a}_{1}, \hat{a}_{2}$ are parallel.

In this case $\hat{d}_{0} = \hat{d}_{1}$ and there are a family of optimal $\hat{r}$'s satisfying the parametric equation

$$
\hat{r}_{\text{opt}} = \frac{\hat{a}_{1}^{0} + \hat{a}_{1}}{|\hat{a}_{1}^{0} + \hat{a}_{1}|} + \lambda \hat{d}_{0}, \quad \text{for } 0 \leq \lambda \leq 2 \frac{\hat{a}_{1}^{0} + \hat{a}_{1}}{|\hat{a}_{1}^{0} + \hat{a}_{1}|} \cdot \hat{d}_{0}. \tag{2.14}
$$

This family corresponds to the points on the chord of the Bloch ball that is parallel to the chord defined by $\hat{a}_{1}^{0}, \hat{a}_{2}^{0}$ (or $\hat{a}_{1}, \hat{a}_{2}$) and that passes through the point on the surface of the ball that is equidistant between $\hat{a}_{1}^{0}$ and $\hat{a}_{1}$. An example is provided in Fig. 2.7.

Case 2: The chords defined by $\hat{a}_{1}^{0}, \hat{a}_{2}^{0}$ and $\hat{a}_{1}, \hat{a}_{2}$ are not parallel.

In this case, the optimal $\hat{r}$ is unique and is given by

$$
\hat{r}_{\text{opt}} = \begin{cases} 
\hat{r}_{\text{max}} & \text{if } |\hat{r}_{\text{max}}| \leq 1 \\
\frac{\hat{a}_{0}^{0} + \hat{a}_{1}}{|\hat{a}_{0}^{0} + \hat{a}_{1}|} & \text{otherwise}
\end{cases}, \tag{2.15}
$$

where

$$
\hat{r}_{\text{max}} = x_{0}^{\text{max}} \hat{d}_{0}^{1} + x_{1}^{\text{max}} \hat{d}_{0}^{1} + x_{2}^{\text{max}} \hat{n}. \tag{2.16}
$$

Here

$$
x_{0}^{\text{max}} = \frac{1}{\gamma_{1}} \hat{a}_{1}^{1} \cdot \hat{d}_{0}^{1} \sqrt{1 - (x_{2}^{\text{max}})^{2}},
$$

$$
x_{1}^{\text{max}} = \frac{1}{\gamma_{0}} \hat{a}_{0}^{0} \cdot \hat{d}_{0}^{1} \sqrt{1 - (x_{2}^{\text{max}})^{2}},
$$

$$
x_{2}^{\text{max}} = \frac{(\hat{a}_{0}^{0} + \hat{a}_{1}) \cdot \hat{n}}{\sqrt{((\hat{a}_{0}^{0} + \hat{a}_{1}) \cdot \hat{n})^{2} + (\gamma_{0} + \gamma_{1})^{2}}}. \tag{2.17}
$$
where \( \gamma_b = \sqrt{1 - (\hat{a}_1^b \cdot \hat{n})^2} \) and where

\[
\begin{align*}
\hat{n} &= \hat{d}_0 \times \hat{d}_1, \\
\hat{d}_b^1 &= \hat{d}_b \times \hat{n}, \\
\hat{d}_b &= \frac{\hat{a}_1^b - \hat{a}_2^b}{|\hat{a}_1^b - \hat{a}_2^b|}.
\end{align*}
\]

Thus, the solution has one of two forms depending on whether the condition \(|\vec{r}^{\text{max}}| \leq 1\) holds or not. If it does not hold, then \(\vec{r}^{\text{opt}} = (\hat{a}_1^0 + \hat{a}_1^1) / |\hat{a}_1^0 + \hat{a}_1^1|\), which is simply the point on the surface of the Bloch ball that is equidistant between \(\hat{a}_1^0\) and \(\hat{a}_1^1\) along the geodesic which connects them (recall that in our labelling convention \(\hat{a}_1^0\) and \(\hat{a}_1^1\) are the closest endpoints of the chords defined by \(\hat{a}_1^0, \hat{a}_1^2\) and \(\hat{a}_1^1, \hat{a}_2^1\)). Fig. 2.6 provides an example of a BC protocol where this is the case. If the condition \(|\vec{r}^{\text{max}}| \leq 1\) does hold, then \(\vec{r}^{\text{opt}} = \vec{r}^{\text{max}}\). We will not attempt to provide a geometrical description of this point in the general case, however Figs. 2.4 and 2.9 provide simple examples of BC protocols where \(|\vec{r}^{\text{max}}| \leq 1\). Note that in these cases, Alice’s optimal cheating strategy requires the use of entanglement.

In situations having a high degree of symmetry, one can easily deduce some of the features of \(\vec{r}^{\text{opt}}\). We present a few such cases.

**Case 2.1:** If the chord defined by \(\hat{a}_1^0\) and \(\hat{a}_2^0\) and the chord defined by \(\hat{a}_1^1\) and \(\hat{a}_1^2\) lie in a plane, then \(\vec{r}^{\text{max}}\) is the point of intersection of the lines containing these chords. If this point falls inside the Bloch ball (\(|\vec{r}^{\text{max}}| \leq 1\), then it represents the optimal density operator. This confirms the results of section 2.5.3. The BB84 BC protocol, illustrated in Fig. 2.4, is an instance of such a case. If the point of intersection falls outside the Bloch ball (\(|\vec{r}^{\text{max}}| > 1\), then the optimal density operator is as described above. The BC protocol that is illustrated in Fig. 2.6 is an instance of such a case.

**Case 2.2:** If the chord defined by \(\hat{a}_1^0\) and \(\hat{a}_2^0\) and the chord defined by \(\hat{a}_1^1\) and \(\hat{a}_2^1\) both pass through the \(\hat{n}\) axis, then \(\vec{r}^{\text{opt}}\) lies along this axis.
A BC protocol where the two sets of states are represented by chords that lie in a plane, but which do not intersect inside the Bloch ball. The optimal density operator is represented by the point that lies equidistant between the two closest chord endpoints on the geodesic which connects them.

**Case 2.3:** If the chord defined by $\hat{a}_1^0$ and $\hat{a}_2^0$ and the chord defined by $\hat{a}_1^1$ and $\hat{a}_2^1$ are parallel to, equidistant from, and on either side of the equatorial plane perpendicular to $\hat{n}$, then $\rho^\text{opt}$ lies in that plane.

If the conditions of cases 2.2 and 2.3 both hold, then $\rho^\text{opt}$ lies at the centre of the Bloch ball. This corresponds to Alice submitting the completely mixed state. An example of such a protocol is provided in Fig. 2.9. Although in the example of this figure the two chords point in orthogonal directions, this is not necessary; it is only necessary that they not be parallel.

The proofs of the results of this section are presented in Appendix B.

**One set contains one element and one set contains two elements** ($n_0 = 1$, $n_1 = 2$)

We now assume that one of the sets $\{\psi_k^0\}_{k=1}^{n_0}$ and $\{\psi_k^1\}_{k=1}^{n_1}$ has only a single element while the other has two. Without loss of generality we may assume that the single element set is the $b = 0$ set, and we denote its unique element by $|\psi^0\rangle$. So in order to unveil a bit
value of 1 Alice can announce either $k = 1$ or $k = 2$ and must then pass Bob's test for $|\psi_k\rangle$. While to unveil a bit value of 0 Alice has no choice but to pass a test for the state $|\psi^0\rangle$.

We first consider the case where $\langle \psi^0 | \psi_1^1 \rangle = \langle \psi^0 | \psi_2^1 \rangle$. This corresponds to case 1 of section 2.6.4 in the limit that $\hat{a}_1^0$ and $\hat{a}_2^0$ converge to a single point $\hat{a}^0$ representing $|\psi^0\rangle$. There is a family of optimal solutions of the form

$$r^{\text{opt}} = \frac{\hat{a}^0 + \hat{a}_1^1}{|\hat{a}^0 + \hat{a}_1^1|} + \lambda \hat{a}_1^1,$$ for $0 \leq \lambda \leq 2$.

This family corresponds to the points on the chord of the Bloch ball that is parallel to the chord defined by $\hat{a}_1^1, \hat{a}_2^1$ and that passes through the point on the surface of the ball that is equidistant between $\hat{a}^0$ and $\hat{a}_1^1$. The BC protocol illustrated in Fig. 2.10 is an example of this case. The case $\langle \psi^0 | \psi_1^1 \rangle \neq \langle \psi^0 | \psi_2^1 \rangle$ corresponds to case 2 of section 2.6.4 in the limit that $\hat{a}_1^0$ and $\hat{a}_2^0$ converge to the point $\hat{a}^0$. In this limit, we find that $|r^{\text{max}}| > 1$. Consequently,

$$r^{\text{opt}} = \frac{\hat{a}^0 + \hat{a}_1^1}{|\hat{a}^0 + \hat{a}_1^1|}.$$ 

**Both sets contain one element** ($n_0 = 1$, $n_1 = 1$)

We now assume there is only a single element in both of the sets, and denote each of these states by $|\psi^b\rangle$. Thus to unveil a bit value of $b$ Alice must pass Bob's test for $|\psi^b\rangle$.

Consider first the possibility that $|\psi^0\rangle$ and $|\psi^1\rangle$ are orthogonal. In this case, no matter what $\rho$ Alice submits, her probability of unveiling either bit is strictly $1/2$.

When $|\psi^0\rangle$ and $|\psi^1\rangle$ are not orthogonal, the situation corresponds to case 2 of section 2.6.4, in the limit that $\hat{a}_1^b$ and $\hat{a}_2^b$ converge to a single point $\hat{a}^b$. In this limit we again find $|r^{\text{max}}| > 1$. Consequently,

$$r^{\text{opt}} = \frac{\hat{a}^0 + \hat{a}_1^1}{|\hat{a}^0 + \hat{a}_1^1|}.$$ 

An example is presented in Fig. 2.8.
2.7 Applications of the results

These results can be applied to the generalized BB84 BC protocol proposed by Aharonov et al. [17]. The protocol is defined by the following states, from which an honest Alice chooses uniformly

\[
|\psi_1^0\rangle = |\theta\rangle, \quad |\psi_2^0\rangle = |-\theta\rangle,
\]
\[
|\psi_1^1\rangle = |\pi/2 - \theta\rangle, \quad |\psi_2^1\rangle = |\pi/2 + \theta\rangle.
\] (2.19)

where $|\theta\rangle = \cos \theta |0\rangle + \sin \theta |1\rangle$ and $\theta$ is some fixed angle satisfying $0 < \theta \leq \frac{\pi}{4}$. The sets of states associated with bits 0 and 1 describe parallel chords on the Bloch ball, as depicted in Fig. 2.7. We therefore have an instance of case 1 of section 2.6.4. It follows that an optimal strategy for Alice is to simply submit $|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$ and tell Bob to test for $|\psi_1^b\rangle$, where $b$ is the bit she wishes to unveil. Another is to submit $|-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$ and to tell Bob to test for $|\psi_2^b\rangle$. So Alice does not need to make use of entanglement in this case. The most general optimal strategy is for Alice to submit $\rho = w |+\rangle \langle +| + (1 - w) |-\rangle \langle -|$, realize the convex decomposition $\{(w, |+\rangle \langle +|), (1 - w, |-\rangle \langle -|)\}$, and
tell Bob to test for $|\psi_1^b\rangle$ ($|\psi_2^b\rangle$) upon obtaining the outcome $|+\rangle$ ($|-\rangle$). Alice's maximum probability of unveiling whatever bit she desires is

$$P_U^{\text{max}} = \frac{1}{2} (1 + \sin 2\theta).$$

Previously, the best known upper bound on this probability was

$$P_U \leq \frac{1}{2} \left(1 + \frac{1}{\cos^2 2\theta} \left(\sqrt{1 + 2\cos^2 2\theta} - 1\right)\right),$$

as can be inferred from the results in section 5 of Ref. [17]. In the case of $\theta = \pi/8$, we find $P_U^{\text{max}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85355$, while the previous best bound was $P_U \leq \frac{\sqrt{2}-1}{2} \approx 0.91421$.

We can now compare this with Bob's maximal probability of estimating Alice's commitment correctly. If Alice follows the honest protocol for committing a bit $b$, she chooses uniformly between $|\psi_1^b\rangle$ and $|\psi_2^b\rangle$ and submits a system in this state. Bob must therefore discriminate between density operators $\rho_0$ and $\rho_1$ defined by $\rho_b = \frac{1}{2} \sum_{k=1}^{2} |\psi_k^b\rangle \langle \psi_k^b|$. His maximum probability of doing so is given by Eq. (2.1). in this case,

$$P_E^{\text{max}} = \frac{1}{2} (1 + \cos 2\theta).$$

It is worth noting that the quantity $\frac{1}{2} \text{Tr} |\rho_0 - \rho_1|$ appearing in Eq. (2.1) is simply half the Euclidean distance between the points in the Bloch ball representing $\rho_0$ and $\rho_1$.

From the above expression for $P_U^{\text{max}}$ and $P_E^{\text{max}}$, we can conclude that there is a trade-off between these quantities of the form

$$(P_U^{\text{max}} - 1/2)^2 + (P_E^{\text{max}} - 1/2)^2 = 1/4. \quad (2.20)$$

At $\theta = 0$, $P_E^{\text{max}} = 1$ and $P_U^{\text{max}} = 1/2$, so that there is no concealment against Bob, but perfect bindingness against Alice (since $P_U^{\text{max}} = 1/2$ for an honest Alice). At $\theta = \pi/4$, ...
Figure 2.8: An illustration of a BC protocol of the form specified in Eq. (2.21), with $\gamma = \pi/4$. The optimal density operator is indicated by the large black sphere. BC protocols of this form achieve the same trade-off between concealment and bindingness as those of the form proposed by Aharonov et al.

$P_E^{\text{max}} = 1/2$ and $P_U^{\text{max}} = 1$, so that the roles of Alice and Bob are reversed. The only choice of $\theta$ leading to a 'fair' protocol is $\theta = \pi/8$. In this case, $P_E^{\text{max}} = P_U^{\text{max}} = \frac{1}{2} + \frac{1}{2\sqrt{2}}$.

Our results also imply that the same trade-off between $P_U^{\text{max}}$ and $P_E^{\text{max}}$ can be achieved with the most simple imaginable BC protocol, namely one wherein Alice submits to Bob one of two non-orthogonal states. Specifically, to commit a bit $b$, an honest Alice sends Bob a qubit in the state $|\psi^b\rangle$, where

\[
|\psi^0\rangle = |0\rangle, \\
|\psi^1\rangle = |\gamma\rangle,
\]

where $\gamma$ is some fixed angle satisfying $0 < \gamma \leq \pi/2$. An example of this protocol is illustrated in Fig. 2.8. This is an instance where $n_0 = 1$ and $n_1 = 1$. which was considered in section 2.6.4. One can infer from the results of that section that Alice’s optimal strategy is to submit the state $|\gamma/2\rangle$ and to announce whatever bit she wishes to unveil. It is straightforward to verify that this protocol has the same properties as the one described above.
It is easy to understand the equivalence of these protocols geometrically. $P^\text{max}_U$ is proportional to the cosine of the angular separation of the endpoints of the polytopes (chords or points) representing the sets of states an honest Alice chooses from. Meanwhile, $P^\text{max}_E$ is proportional to the Euclidean distance between the midpoints of these polytopes. It is easy to see from Figs. 2.7 and 2.8 that if the endpoints have the same angular separation, then the midpoints have the same Euclidean separation.

Interestingly, it turns out that any protocol satisfying the conditions of cases 2.2 and 2.3 of section 2.6.4 also yields exactly the same trade-off between $P^\text{max}_U$ and $P^\text{max}_E$. Specifically, one can use any protocol of the form

$$
|\psi^0_1\rangle = |\theta, 0\rangle, |\psi^0_2\rangle = |\theta, 0\rangle,
|\psi^1_1\rangle = |\pi/2 - \theta, \phi\rangle, |\psi^1_2\rangle = |\pi/2 + \theta, -\phi\rangle,
$$

where $|\theta, \phi\rangle = \cos \theta |0\rangle + e^{i\phi} \sin \theta |1\rangle$ and $\theta$ and $\phi$ are fixed angles satisfying $0 < \theta \leq \pi/4$, $0 < \phi \leq \pi/2$. Fig. 2.9 depicts an example of such a protocol. Geometrically, $P^\text{max}_U$ is no longer given by the angle between the endpoints of the two polytopes representing the states an honest Alice chooses from but rather the angle between the endpoints of these polytopes and the closest endpoints of the polytopes representing the elements of the convex decomposition that Alice realizes. Nonetheless, the fact that the latter angle is simply half of the former angle ensures that $P^\text{max}_U$ is the same. The only difference is that Alice's optimal strategy in this case requires the use of entanglement.

Finally, we consider a protocol wherein there is a single state associated with committing a bit 0 but two states associated with committing bit 1, specifically

$$
|\psi^0\rangle = |0\rangle,
|\psi^1_1\rangle = |\alpha\rangle, |\psi^1_2\rangle = |\alpha\rangle,
$$

(2.23)
Figure 2.9: An illustration of a BC protocol of the form specified in Eq. (2.22), with $\theta = \pi/8$ and $\phi = \pi$. The optimal density operator in this case lies at the origin. Depending on which bit Alice desires to unveil, she realizes the convex decomposition parallel to one or the other of the two chords.

where $\alpha$ is some fixed angle satisfying $0 < \alpha \leq \pi/2$. An example of this protocol is provided in Fig. 2.10. It is an instance where $n_0 = 1$ and $n_1 = 2$, which was considered in section 2.6.4, with $\langle \psi^0 | \psi_1^1 \rangle = \langle \psi^0 | \psi_2^1 \rangle$. From the results of that section, we can infer that there are a family of optimal coherent attacks of the following form. Alice submits a density operator of the form $\rho = w |\alpha/2\rangle \langle \alpha/2| + (1 - w) |\alpha/2\rangle \langle -\alpha/2|$. If she decides to try to unveil bit 0, she simply announces this to Bob. If she decides to try to unveil bit 1, she realizes the convex decomposition $\{(w, |\alpha/2\rangle \langle \alpha/2|), (1 - w, |\alpha/2\rangle \langle -\alpha/2|)\}$, and upon obtaining the outcome $|\alpha/2\rangle \langle |\alpha/2|$, tells Bob to test for $|\alpha\rangle \langle |\alpha|$). Alice's maximum probability of unveiling whatever bit she desires in this case is

$$P_U^{\text{max}} = \frac{1}{2} + \frac{1}{2} \cos \alpha.$$  

Meanwhile, from Eq. (2.1), we can infer that Bob's maximum probability of correctly estimating Alice's commitment is

$$P_E^{\text{max}} = \frac{1}{2} + \frac{1}{2} \sin^2 \alpha.$$
Figure 2.10: An illustration of a BC protocol of the form specified in Eq. (2.23), with \( \alpha = \arccos((\sqrt{5} - 1)/2) \). There is a family of optimal density operators lying along the chord indicated in grey. BC protocols of this form achieve a better trade-off between concealment and bindingness than those of the form proposed by Aharonov et al.

The trade-off between \( P^\text{max}_U \) and \( P^\text{max}_E \) is

\[
2 \left( P^\text{max}_U - \frac{1}{2} \right)^2 + \left( P^\text{max}_E - \frac{1}{2} \right) = \frac{1}{2}.
\]

(2.24)

A 'fair' protocol has \( P^\text{max}_U = P^\text{max}_E = \frac{1}{2} + \frac{\sqrt{5} - 1}{4} \approx 0.80902 \).

From a comparison of the trade-offs (2.19) and (2.24), it is easy to verify that a protocol which uses the states (2.23) achieves, for a given bindingness (a given \( P^\text{max}_U \)), a concealment that is greater (and thus a \( P^\text{max}_E \) that is smaller) than the concealment that can be achieved in a protocol using the states (2.19), (2.21) or (2.22).

This point is easy to see geometrically. We compare the states (2.23) with the states (2.21) for simplicity. From an inspection of Figs. 2.8 and 2.10 it is easy to see that if the endpoints of the polytopes defined by the two protocols have the same angular separation, the midpoints do not have the same Euclidean separation - the separation is smaller for a BC protocol defined by the states (2.23).

An obvious question to ask at this point is whether the trade-off relation of Eq. (2.24) is optimal, in the sense that the concealment against Bob is maximized for a given
bindingness against Alice. In chapter 3, we show that it is optimal among a certain class of protocols (which includes the generalized BB84 protocols) that can be implemented using a single qubit. It is also shown that a better trade-off can be achieved with a BC protocol that can be implemented using a single qudit, that is, a three-level system. The protocol we suggest in chapter 3 is not a generalized BB84 BC protocol, however, an equivalent protocol that is of the generalized BB84 form has been proposed by Ambainis [47].

2.8 Conclusions

We have formulated the problem of optimizing coherent attacks in generalized BB84 BC protocols in terms of a well known theorem of Hughston, Jozsa and Wootters. We have found that there is a mapping between this problem and one of state estimation. Specifically, we have shown that the convex decomposition of a fixed density operator that is optimal for successfully preparing one of a set of states is related in a simple way to the POVM measurement that is optimal for discriminating among certain transformations of these states.

We have identified Alice’s optimal coherent attack for a class of generalized BB84 BC protocols that can be implemented using a single qubit. From these results we have determined the degree of bindingness that can be achieved in the BC protocol proposed by Aharonov et al., improving upon the best previous upper bound. This enables us to identify the trade-off between the degree of concealment and the degree of bindingness for this protocol. It has also led us to identify several qubit protocols that achieve the same trade-off as the proposal of Aharonov et al., as well as a qubit protocol that achieves a better trade-off.

In optimizing over Alice’s strategies, we have relied on the Bloch ball representation of quantum states. This provides a convenient geometrical picture of a coherent attack.
Although this representation can be generalized to higher dimensions \[48\], it is unlikely that such simple geometric pictures can be provided in the general case. In any event, there remain many questions to be answered even for qubit protocols, for which this approach is likely to provide some insight. For instance, one can use it to consider qubit BC protocols that are \emph{not} generalizations of the BB84 BC protocol.

In the next chapter, we turn to the optimization of coherent attacks in a class of BC protocols that is larger than the class of generalized BB84 protocols, and we investigate the trade-offs between concealment and bindingness that can be achieved in this larger class.
Chapter 3

Degrees of bindingness and concealment in quantum bit commitment protocols

3.1 Introduction

Recall that in a bit commitment (BC) protocol, one seeks to have Alice submit an encoded bit of information to Bob in such a way that Bob cannot reliably identify the bit before Alice decodes it for him, and Alice cannot reliably change the bit after she has submitted it. In other words, Bob is interested in binding Alice to some commitment, and Alice is interested in concealing this commitment from Bob. Mayers [20], and independently Lo and Chau [21], have shown that a BC protocol that is both concealing and binding is impossible [49]. Nonetheless, it is possible to devise a BC protocol that is both partially concealing and partially binding, that is, one wherein if Alice is honest then the probability that Bob can estimate her commitment correctly is strictly less than 1, and if Bob is honest then the probability that Alice can unveil whatever bit she desires is strictly less than 1. This chapter addresses the problem of determining the optimal
degrees of concealment and bindingness that can be achieved simultaneously in quantum bit commitment protocols.

Building upon the work of Mayers and Lo and Chau, we establish an upper bound on the degrees of concealment and bindingness for all BC protocols. It is unclear at this time whether or not this upper bound can be saturated. Nonetheless, we are able to provide a saturable upper bound for a more restricted class of BC protocols, namely protocols wherein Alice initially holds all of the systems that play a role in the commitment phase of the protocol. We also introduce a new kind of BC protocol that achieves this maximum. The protocol essentially consists of Alice preparing two systems in an entangled state, submitting one half to Bob at the commitment phase, and submitting the other half at the unveiling phase. We show that in such protocols the maximum achievable degree of bindingness is related in a simple way to the fidelity between the reduced density operators for the systems held by Bob at the end of the commitment phase.

BC appears as a primitive in the protocols of many different cryptographic tasks between mistrustful parties. As such, the kinds of security that can be achieved in BC has implications for the kinds of security that can be achieved in these other tasks. Here we consider only the implications of our results to the task of coin tossing [14].

3.2 Degrees of concealment and bindingness

In order to optimize over all BC protocols, we need to provide a precise definition of BC. We will provide a definition that is strictly operational, that is, one which only makes reference to the experimental operations carried out by the parties, and not to any concepts that are particular to a physical theory. This seems to us to be the most sensible way of proceeding for any information processing task, since such tasks can be defined independently of their physical implementation and consequently of any physical theory describing this implementation. Among other benefits, this approach allows one to
characterize a physical theory by the type of protocols which can be securely implemented within a universe described by that theory.

A BC protocol is a cryptographic protocol between two mistrustful parties. It can be defined in terms of the characteristics of these parties' honest \textit{(i.e., non-cheating)} strategies. We call the two parties Alice and Bob, and assume that Alice is the one making the commitment. The protocol is divided into three intervals, called the commitment phase, the holding phase and the unveiling phase. During the commitment phase, Alice and Bob engage in some number of rounds of communication, with at least one communication from Alice to Bob. The period after the end of the commitment phase and prior to the beginning of the unveiling phase is called the holding phase, and may be of arbitrary duration. During the unveiling phase, there is again some number of rounds of communication, with at least one communication from Alice to Bob. At the end of the unveiling phase, an honest Bob decides, based on the outcomes of any measurements he has performed during the protocol, whether the result of the protocol is '0', '1' and 'fail', corresponding respectively to Alice unveiling a 0, Alice unveiling a 1 and Alice being caught cheating. The protocol specifies the sequence of actions an honest Alice performs in order to commit to a bit $b$, and guarantees that if she follows the actions for committing a bit $b$ then an honest Bob finds that the result of the protocol is '$b$' with certainty.

To discuss the security of BC protocols, it is useful to introduce two quantities which we shall call Alice's \textit{control} and Bob's \textit{information gain}. These quantities are defined under the assumption that the other party is honest, and depend on the sequence of actions performed by the party in question. Alice's control is meant to quantify the extent to which she can influence (after the commitment phase) the result of Bob's measurement beyond what she could accomplish by following the honest protocol. Bob's information gain is meant to quantify his ability to estimate Alice's commitment (prior to the unveiling phase) beyond what he could accomplish by following the honest protocol.
We now present the specific measures of control and information gain which we make use of in this chapter. We assume for simplicity that Bob has no prior information on which bit Alice has committed, and that Alice is as likely to wish to unveil a bit 0 as she is to wish to unveil a bit 1. We take our measure of Bob's information gain for the strategy \( S^B \), which we denote by \( G(S^B) \), to be the difference between his probability of estimating Alice's commitment correctly when he implements \( S^B \) and this probability when he is honest,

\[
G(S^B) = P_E(S^B) - 1/2.
\]

We take our measure of Alice's control for the strategy \( S^A \), which we denote by \( C(S^A) \), to be the difference between her probability of unveiling whatever bit she desires when she implements \( S^A \) and this probability when she is honest,

\[
C(S^A) = P_U(S^A) - 1/2.
\]

It follows that \( G(S^B) \) and \( C(S^A) \) vary between 0 and 1/2. Note that in chapter 2 we described our results in terms of \( P_E \) and \( P_U \) rather than \( G \) and \( C \), but since these quantities only differ by a constant offset, the two approaches are equivalent.

We quantify the degrees of concealment and bindingness in a BC protocol by Bob's maximum information gain and Alice's maximum control, defined respectively by

\[
G^{\text{max}} \equiv \max_{S^B} G(S^B).
\]

\[
C^{\text{max}} \equiv \max_{S^A} C(S^A).
\]

A protocol is said to be partially concealing if Bob's maximum information gain is strictly less than complete information gain, \( G^{\text{max}} < 1/2 \); it is said to be perfectly concealing if his information gain is zero, \( G^{\text{max}} = 0 \); finally, it is said to be arbitrarily concealing or simply concealing if his information gain can be made arbitrarily small by increasing
the value of a security parameter $N$, that is, $G^\text{max} \leq \varepsilon$, where $\varepsilon \to 0$ as $N \to \infty$ [51]. Similar definitions hold for the degrees of security against Alice. A protocol is said to be partially binding if Alice’s maximal control is strictly less than complete control, $C^\text{max} < 1/2$; it is said to be perfectly binding if her control is zero, $C^\text{max} = 0$; finally, it is said to be arbitrarily binding or simply binding if her control can be made arbitrarily small by increasing the value of a security parameter $N$, that is, $C^\text{max} \leq \delta$, where $\delta \to 0$ as $N \to \infty$.

If a degree of security (such as concealment or bindingness) can be guaranteed by assuming only the laws of physics (and the integrity of a party’s laboratory), then it is said to hold unconditionally. We shall only be concerned with unconditional security here. Thus, every time we assign some degree of security (such as concealment or bindingness) to a protocol, it is implied that the protocol has this feature unconditionally.

To understand the degree to which a protocol can be made concealing or binding we must answer the following questions:

- What is Bob’s maximal information gain, and what strategy achieves this maximum? That is, find $G^\text{max}$, and find $S_B^\text{max}$ such that $G(S_B^\text{max}) = G^\text{max}$.
- What is Alice’s maximal control, and what strategy achieves this maximum? That is, find $C^\text{max}$, and find $S_A^\text{max}$ such that $C(S_A^\text{max}) = C^\text{max}$.

In chapter 2, we provided answers to these questions for BC protocols that are generalizations of the BB84 BC protocol [19]. In this chapter, we provide the answers for a different type of BC protocol, which we call a purification BC protocol.

The above questions involve an optimization over strategies. We will also be interested in optimizing over protocols. Specifically, we wish to answer the following question:

- For a given class of protocols, what is the minimum Alice’s maximum control can be made for a given value of Bob’s maximum information gain, and which protocol
in the class achieves this minimum? In other words, denoting protocols by \( \mathcal{P} \), the given class of protocols by \( \mathcal{K} \), and the subset of this class associated with \( G^{\max} \) by \( \mathcal{K}(G^{\max}) \), find \( \min_{\mathcal{P} \in \mathcal{K}(G^{\max})} C^{\max}(\mathcal{P}) \) and find \( \mathcal{P}^{\text{opt}} \) such that \( C^{\max}(\mathcal{P}^{\text{opt}}) = \min_{\mathcal{P} \in \mathcal{K}(G^{\max})} C^{\max}(\mathcal{P}) \).

If this question can be answered for every value of \( G^{\max} \), then one obtains a curve in the \( G^{\max}-C^{\max} \) plane. Moreover, if this curve is monotonically decreasing then it is identical to what would have been obtained by minimizing Bob’s maximum information gain for a given value of Alice’s maximum control. In this case, we call the curve the *optimal trade-off relation* between \( C^{\max} \) and \( G^{\max} \). Specifying this relation for a given class of protocols is a convenient way of expressing the maximum degrees of concealment and bindingness that can be achieved with such protocols.

In this chapter, we determine a lower bound on the optimal trade-off relation between \( C^{\max} \) and \( G^{\max} \) for all BC protocols. Unfortunately, we have not determined whether this lower bound is saturable or not. However, we do find the optimal trade-off relation for a restricted class of BC protocols, which we call *Alice-supplied* BC protocols. The generalized BB84 BC protocols and the purification BC protocols mentioned above both fall into this class. In fact, we show that the purification BC protocols are optimal within this class. These protocols will be defined precisely in the next section.

### 3.3 BC protocols

In the previous section, we provided an operational description of the most general form of a BC protocol. We must now specify the quantum mechanical model we shall adopt in describing any such protocol. We make use of the following general quantum model for cryptographic protocols implemented between two mistrustful parties [20]. The Hilbert space required to describe the protocol is the tensor product of the Hilbert spaces for all the systems that play a role in the protocol. Every action taken by a party in their
laboratory corresponds to that party performing a unitary operation on the systems in their possession. Every communication corresponds to a party sending some subset of the systems in their possession to the other party (it follows that the mere transmission of information from one party to the other does not change the quantum state of the total system, but does change the Hilbert space upon which the parties can implement their unitary operations). It is assumed that the total system is initially in a pure state. Measurements are only made at the end of the protocol.

It has been previously argued [20] that this model is completely general. It incorporates the possibility of random choices and measurements during the protocol, since these can always be kept at the quantum level until the end without any loss of generality. A random choice is performed at the quantum level by implementing a unitary transformation that is conditioned upon the state of an ancilla prepared initially in a particular superposition of states. Measurements are performed at the quantum level by unitarily coupling the system to be measured to an ancilla that is prepared in some fixed initial pure state.

In the case of BC, the most general protocol may involve many rounds of communication during the commitment phase. Denoting the number of rounds by $n$, denoting Alice's honest sequence of operations for committing a bit $b$ by $\{W_{b,1}, \ldots, W_{b,n}\}$, and denoting Bob's honest sequence of operations by $\{W'_{1}, \ldots, W'_{n}\}$, the total unitary operation they jointly implement is

$$W_b \equiv W'_{n}W_{b,n} \cdots W'_{2}W_{b,2}W'_{1}W_{b,1}.$$ 

The transmissions that occur in each round will determine the Hilbert space over which $W_{b,i}$ and $W'_{i}$ act non-trivially. Thus, despite the fact that we have assumed that Alice implements the first unitary operation, this operation could be trivial and it remains arbitrary which party is first to submit a system to the other party. If the initial state of
all systems is denoted by $|\psi_{\text{init}}\rangle$, then the state at the holding phase if both parties are honest is

$$|\psi_b\rangle \equiv W_b |\psi_{\text{init}}\rangle.$$ 

It follows that the reduced density operator for Bob's system at the holding phase, assuming both parties are honest, is

$$\rho_b = \text{Tr} (|\psi_b\rangle \langle \psi_b|),$$

where the trace is over all the systems that end up in Alice's possession at the holding phase.

During the unveiling phase, a similar process occurs. Denoting the number of rounds by $m$, denoting Alice's honest sequence of operations given that she committed to bit $b$ by $\{V_{b,1}, ..., V_{b,n}\}$, and denoting Bob's honest sequence of operations by $\{V'_{1}, ..., V'_{n}\}$, the total unitary operation they jointly implement is

$$V_b \equiv V'_{n}V_{b,n} \cdots V'_{2}V_{b,2}V'_{1}V_{b,1}.$$ 

Thus, if both parties are honest, the state of the total system at the end of the unveiling phase is

$$|\psi_b^{\text{unv}}\rangle \equiv V_b |\psi_b\rangle.$$  \hspace{1cm} (3.1)

The protocol ends with Bob performing a three-outcome projective measurement $\{\Pi_0, \Pi_1, \Pi_{\text{fail}}\}$ on the systems in his possession. If both parties are honest, then whenever Alice commits to a bit $b$, the measurement must have outcome $b$ with probability 1. This implies that $|\psi_0^{\text{unv}}\rangle$ and $|\psi_1^{\text{unv}}\rangle$ must be orthogonal,

$$\langle \psi_0^{\text{unv}} | \psi_1^{\text{unv}} \rangle = 0.$$
and that $|\psi^{\text{inv}}_b\rangle$ must be an eigenstate of $\Pi_b$ with eigenvalue 1,

$$\Pi_b |\psi^{\text{inv}}_b\rangle = |\psi^{\text{inv}}_b\rangle.$$  \hspace{1cm} (3.2)

As mentioned earlier, we will be interested in a restricted class of BC protocols, which we call *Alice-supplied* BC protocols. These protocols impose no restrictions on the details of the unveiling phase and may involve an arbitrary number of rounds of communication between Alice and Bob during the commitment phase. However, it is required that *all* of the systems that Bob makes use of during the commitment phase are supplied by Alice. The class of Alice-supplied BC protocols includes the generalized BB84 BC protocols, defined in chapter 2, as well as the purification BC protocols defined below.

An example of a protocol that falls *outside* this class is one wherein at the beginning of the commitment phase Bob submits to Alice a system that is entangled with one he keeps in his possession, and Alice encodes her commitment in the unitary transformation she performs upon this system before resubmitting it to Bob. Another example of such a protocol is one wherein during the commitment phase Bob uses ancillas that Alice did not supply in order to make a random choice or perform a measurement.

We now provide a precise definition of a purification BC protocol.

**A purification BC protocol.** Such a protocol makes use of just two systems, which we shall call the token system and the proof system (since one is the token of Alice's commitment and the other is the proof of her commitment). These are associated with Hilbert spaces $\mathcal{H}_p$ and $\mathcal{H}_t$. A purification BC protocol also specifies two orthogonal states $|\chi_0\rangle$ and $|\chi_1\rangle$ defined on $\mathcal{H}_p \otimes \mathcal{H}_t$. The honest actions are as follows.

1. At the commitment phase, Alice prepares the two systems in the state $|\chi_b\rangle$ in order to commit to bit $b$, and sends the token system to Bob.

2. At the unveiling phase, Alice sends the proof system to Bob, and Bob performs a measurement of the projector-valued measure $\{\Pi_0, \Pi_1, \Pi_{\text{fail}}\}$, where $\Pi_b = |\chi_b\rangle \langle \chi_b|$. 

So we see there is only a single communication from Alice to Bob during both the commitment and the unveiling phases. In the notation of the general model presented above, $W_b$ transforms $|\psi_{\text{init}}\rangle$ to $|\psi_b\rangle = |\chi_b\rangle$, and $V_b = I$ so that $|\psi_b^{\text{inv}}\rangle = |\psi_b\rangle = |\chi_b\rangle$.

We call this a purification BC protocol, since at the unveiling phase an honest Alice is required to provide Bob with a purification of the state that he received from her during the commitment phase.

### 3.4 Measures of distinguishability for density operators

Two measures of the distinguishability of density operators will be important in the present work: the trace distance and the fidelity, defined respectively by [7]

$$D(\rho, \sigma) = \frac{1}{2} \text{Tr} |\rho - \sigma|,$$

and

$$F(\rho, \sigma) = \text{Tr} |\sqrt{\rho} \sqrt{\sigma}|,$$

where $|A| = \sqrt{A^\dagger A}$.

We will find the following relations between these two measures to be very useful. For any two density operators, the fidelity and the trace distance satisfy [7]

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma),$$  \hspace{1cm} (3.3)

and

$$D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}$$  \hspace{1cm} (3.4)
The second inequality is saturated for any pair of pure states, that is,

\[ D(\ket{\psi}, \ket{\chi}) = \sqrt{1 - F(\ket{\psi}, \ket{\chi})^2}, \]  

(3.5)

for all \( \ket{\psi} \) and \( \ket{\chi} \). A stronger lower bound for the trace distance between \( \rho \) and \( \sigma \) exists if one of the density operators is pure. Specifically,

\[ 1 - F(\rho, \ket{\psi})^2 \leq D(\rho, \ket{\psi}). \]  

(3.6)

This stronger lower bound also applies to the mixed states of qubits. More precisely, we have the following result.

**Lemma 1** For pairs of density operators \( \rho, \sigma \) whose supports lie in a single 2-dimensional Hilbert space,

\[ 1 - F(\rho, \sigma)^2 \leq D(\rho, \sigma). \]

The proof of this is presented in appendix C. All of the above inequalities can be saturated. Explicit examples will be presented in section 3.6.2.

Finally, we present some properties of the fidelity that will be useful for the present investigation. Uhlmann's theorem [52] states that the fidelity between two density operators is equal to the overlap of two maximally parallel purifications of these density operators. Thus, if \( \rho \) and \( \sigma \) are density operators on a Hilbert space \( \mathcal{H} \), \( \ket{\psi} \) and \( \ket{\chi} \) are arbitrary purifications of \( \rho \) and \( \sigma \) on \( \mathcal{H}' \otimes \mathcal{H} \), and \( U \) is a unitary transformation on \( \mathcal{H}' \), then

\[ F(\rho, \sigma) = \max_U |\langle \psi | U \otimes I \ket{\chi}|. \]  

(3.7)

Another critical property is given by the following lemma.
Lemma 2 The fidelity satisfies

$$\max_{\rho} \left( F(\rho, \sigma)^2 + F(\rho, \omega)^2 \right) = 1 + F(\sigma, \omega).$$

The proof of this can be found in the derivation of Eq. (3.11) from Eq. (3.9) in section 3.6.1 and by making use of Uhlmann’s theorem.

3.5 Optimizing over all BC protocols

In this section, we demonstrate an upper bound on the simultaneous degrees of concealment and bindingness (hence a lower bound on $C^\text{max}$ and $C^\text{max}$) for any BC protocol. It should be noted that the main ideas that go into the proof of this result are present in the work of Mayers [20] and Lo and Chau [14].

Theorem 1 In any BC protocol,

\[
\begin{align*}
\text{i) } C^\text{max} & \geq \frac{1}{2} D(\rho_0, \rho_1), \\
\text{ii) } C^\text{max} & \geq \frac{1}{2} F(\rho_0, \rho_1)^2.
\end{align*}
\]

Proof. We begin by proving (i). To analyze security against Bob, we assume that Alice is honest. Suppose that Bob uses a strategy wherein he acts honestly throughout the commitment phase. In this case, the state of the total system at the end of this phase will be $|\psi_0\rangle$ or $|\psi_1\rangle$, depending on Alice’s commitment. The reduced density operators for Bob’s system will be $\rho_0$ or $\rho_1$. Now suppose that during the holding phase Bob does the measurement which optimally discriminates between $\rho_0$ and $\rho_1$. It is a well-known result of state estimation theory [40][41] that his information gain in this case will be

$$G = \frac{1}{2} D(\rho_0, \rho_1).$$
Bob's maximum information gain may be greater than this value, since it may be beneficial for him to also cheat during the commitment phase (for instance, if the reduced density operators on Bob's systems are more easily discriminated at some point during the commitment phase than they are at the holding phase). Bob's maximum information gain cannot, however, be less than this bound. This establishes (i).

We now prove (ii). To analyze security against Alice, we can assume that Bob is honest. Suppose that Alice uses the following strategy. During the commitment phase, she follows the honest protocol for committing a bit 0, so that the total system is in the state $|\psi_0\rangle$ at the holding phase. If Alice wishes to unveil a bit 0, she acts honestly for the rest of the protocol, while if she wishes to unveil a bit 1, she applies a unitary transformation $U^{\text{max}}$ to the systems in her possession just prior to the unveiling phase, and thereafter acts honestly. $U^{\text{max}}$ is chosen such that

$$\langle \psi_1 | U^{\text{max}} \otimes I | \psi_0 \rangle = \max_U \langle \psi_1 | U \otimes I | \psi_0 \rangle. \quad (3.8)$$

The probability that Alice succeeds at unveiling a bit 0 when she attempts to do so is unity, $P_{10} = 1$, since she has simply followed the honest protocol for committing a 0. The probability that Alice succeeds at unveiling a bit 1 when she attempts to do so is

$$P_{U1} = \text{Tr} \left( \Pi_1 V_1 (U^{\text{max}} \otimes I) |\psi_0\rangle \langle \psi_0 | (U^{\text{max}})^* \otimes I) V_1^* \right).$$

Now since the state $|\psi_1^{\text{inv}}\rangle = V_1 |\psi_1\rangle$ is an eigenstate of $\Pi_1$ with eigenvalue 1 (see Eq. (3.2)), one can write

$$\Pi_1 = |\psi_1^{\text{inv}}\rangle \langle \psi_1^{\text{inv}} | + \Gamma_1,$$

for some non-negative operator $\Gamma_1$, orthogonal to $|\psi_1^{\text{inv}}\rangle \langle \psi_1^{\text{inv}} |$. It follows that

$$P_{U1} \geq |\langle \psi_1^{\text{inv}} | V_1 (U^{\text{max}} \otimes I) | \psi_0 \rangle|^2$$
Since we are assuming that Alice is equally likely to wish to unveil a 0 as a 1, her probability of unveiling the bit of her choosing satisfies

\[ P_U = \frac{1}{2} P_{U0} + \frac{1}{2} P_{U1} \geq \frac{1}{2} + \frac{1}{2} |\langle \psi_1 | U^{\text{max}} \otimes I | \psi_0 \rangle|^2. \]

Recalling the definition of $U^{\text{max}}$ (Eq. (3.8)), and making use of Uhlmann's theorem (Eq. (3.7)), we conclude that Alice's control for this particular strategy satisfies

\[ C \geq \frac{1}{2} F(\rho_0, \rho_1)^2. \]

Alice's maximum control may be greater than this bound, since she may be able to cheat during the commitment and unveiling phases as well, but it cannot be less. This establishes (ii). □

**Corollary 1** In any BC protocol, the optimal trade-off between $G^{\text{max}}$ and $C^{\text{max}}$ is a curve satisfying

\[ 2G^{\text{max}} + \sqrt{2C^{\text{max}}} \geq 1. \]

(the lower bound corresponds to curve I in Fig. 3.1).

**Proof:** This follows from Theorem 1 and Eq. (3.3). □

The Mayers-Lo-Chau theorem [20][21] states that it is impossible to have a BC protocol that is both arbitrarily concealing and arbitrarily binding, that is, one for which $G^{\text{max}} \leq \varepsilon$ and $C^{\text{max}} \leq \delta$ for arbitrarily small $\delta$ and $\varepsilon$. This clearly follows from Corollary 1. However, Corollary 1 says *more* than this, since it also sets a lower bound on the extent to which any BC protocol can be partially concealing and partially binding. Thus,
Figure 3.1: Curve I is a lower bound for the trade-off relation between \( C^{\text{max}} \) and \( G^{\text{max}} \) for any BC protocol. The other curves are the optimal trade-off relations for Alice-supplied BC under different restrictions on \( \rho_0 \) and \( \rho_1 \): (II) no restrictions; (III) both qubit states or not both mixed states; and (IV) both pure states. A, B, C and D correspond to the points along these curves where the protocol is fair, i.e. \( C^{\text{max}} = G^{\text{max}} \).
in addition to being able to rule out the possibility of a BC protocol with $G^\text{max}$ and $C^\text{max}$ arbitrarily close to the origin in Fig. 3.1, one can rule out the possibility of a BC protocol anywhere below curve I of Fig. 3.1. The best one can hope for is a BC protocol with $2G^\text{max} + \sqrt{2C^\text{max}} = 1$ (curve I of Fig. 3.1). In particular, the best fair BC protocol one can hope for has $C^\text{max} = G^\text{max} = \frac{3 - \sqrt{5}}{4} \approx 0.19098$ (point A in Fig. 3.1).

We do not settle the question of whether there exists a protocol for which Alice's maximal control and Bob's maximal information gain achieve the lower bounds of Theorem 1 simultaneously. Such a protocol would have to be such that Bob could not get any more information by cheating during the commitment phase than he can by cheating during the holding phase, and such that Alice could not get any more control by cheating during the commitment phase or the unveiling phase than she can by cheating during the holding phase. It seems to us that such a protocol is unlikely to exist.

### 3.6 Optimizing over Alice-supplied BC protocols

#### 3.6.1 Optimal degrees of concealment and bindingness

The main results of this chapter are:

**Theorem 2** In Alice-supplied BC protocols,

\begin{align*}
i) \quad G^\text{max} &\geq \frac{1}{2} D(\rho_0, \rho_1) \\
ii) \quad C^\text{max} &\geq \frac{1}{2} F(\rho_0, \rho_1)
\end{align*}

and

**Theorem 3** Purification BC protocols saturate the bounds in Theorem 2.

**Proof of Theorem 2.** Inequality (i) follows trivially from theorem 1, since if $G^\text{max} \geq \frac{1}{2} D(\rho_0, \rho_1)$ for all BC protocols then clearly $G^\text{max} \geq \frac{1}{2} D(\rho_0, \rho_1)$ for any Alice-supplied
Inequality (ii), on the other hand, is stronger than theorem 1. To prove it, we must consider Alice’s most general cheating strategy. Without loss of generality, we can assume that she keeps all of her cheating actions at the quantum level. During the commitment phase, Alice can cheat by implementing a sequence of unitary operations \( \{W_1, \ldots, W_n\} \) different from the honest sequence. She can cheat at the end of the holding phase by implementing a unitary transformation \( U_b \otimes I \) that depends on the bit \( b \) she would like to unveil. Finally, she can cheat during the unveiling phase by implementing a sequence of unitary operations \( \{\tilde{V}_{b,1}, \ldots, \tilde{V}_{b,n}\} \) that depends on the bit \( b \) she would like to unveil and that is different from the honest sequence. The maximum probability of Alice unveiling the bit of her choosing is therefore given by

\[
P_{\text{U}}^{\text{max}} = \frac{1}{2} \max_{\{w_1, \ldots, w_n\}} \sum_{b \in \{0,1\}} \max_{\{\tilde{v}_{b,1}, \ldots, \tilde{v}_{b,n}\}} \text{Tr}(\Pi_b \tilde{V}_b (U_b \otimes I) \tilde{W} |\psi_{\text{init}}\rangle \langle \psi_{\text{init}}| \times \tilde{W}^\dagger (U_b^\dagger \otimes I) \tilde{V}_b^\dagger)\]

where

\[
\tilde{W} \equiv W_n^\dagger \tilde{W}_n \cdots W_2^\dagger \tilde{W}_2 W_1^\dagger \tilde{W}_1, \quad \text{and}
\]

\[
\tilde{V}_b \equiv V_n^\dagger \tilde{V}_{b,n} \cdots V_2^\dagger \tilde{V}_{b,2} V_1^\dagger \tilde{V}_{b,1}.
\]

\( \tilde{W} \) and \( \tilde{V}_b \) are the total unitary operations that Alice and Bob jointly implement given that Bob is honest and Alice cheats.

We begin by optimizing over Alice’s cheating strategy during the commitment phase. It turns out that the assumption of an Alice-supplied protocol allows us to replace the maximization over \( \{W_1, \ldots, W_n\} \) by a maximization over all unitary operations on the total system. This means that Alice has as much cheating power in an arbitrary Alice-
supplied protocol as she does in a protocol where Bob does not play any role in the commitment phase. The reason is that Alice can bring about any unitary operation \( W \) by implementing the sequence of operations

\[
\tilde{W}_1 = (W'_n \cdots W'_1)^{-1} W \\
\tilde{W}_i = I \text{ for } i \neq 1
\]

This result only applies for Alice-supplied BC protocols, since Alice must initially have access to all the systems that will appear in the commitment phase in order to implement \( \tilde{W}_1 \). We can conclude that

\[
P_U^{\text{max}} = \frac{1}{2} \max_{\mathcal{W}} \sum_{b \in \{0,1\}} \max_{\mathcal{V}_b, \cdots, \mathcal{V}_{b,n}} \max_{\mathcal{U}_b} \text{Tr}(\Pi_b \tilde{V}_b (U_b \otimes I) W |\psi_{\text{init}}\rangle \langle \psi_{\text{init}}| \\
\times W^\dagger (U_b^\dagger \otimes I) \tilde{V}_b^\dagger)
\]

We now consider the unveiling measurement. Eq. (3.2) implies that the honest state at the end of the unveiling phase, \( |\psi_b^{\text{unv}}\rangle \) must be an eigenstate of \( \Pi_b \). Thus,

\[
\Pi_b = |\psi_b^{\text{unv}}\rangle \langle \psi_b^{\text{unv}}| + \Gamma_b.
\]

for some non-negative operator \( \Gamma_b \). It follows that

\[
P_U^{\text{max}} \geq \frac{1}{2} \max_{\mathcal{W}} \sum_{b \in \{0,1\}} \max_{\mathcal{V}_b, \cdots, \mathcal{V}_{b,n}} \max_{\mathcal{U}_b} \left| \langle \psi_b^{\text{unv}} | \tilde{V}_b (U_b \otimes I) W |\psi_{\text{init}}\rangle \right|^2.
\]
Clearly the maximum over \{\tilde{V}_{b,1}, \ldots, \tilde{V}_{b,n}\} must be greater than or equal to the value for \{V_{b,1}, \ldots, V_{b,n}\}, the honest sequence of operations for unveiling bit \(b\). Thus,

\[
P_{U}^{\text{max}} \geq \frac{1}{2} \max_{W} \sum_{b \in \{0,1\}} \max_{U_b} |\langle \psi_b^{\text{inv}} | V_b (U_b \otimes I) W | \psi_{\text{init}} \rangle|^2.
\]

Since \(W\) varies over all unitary operators, we can write \(|\psi\rangle = W |\psi_{\text{init}}\rangle\) and vary over all \(|\psi\rangle\). Making use of the fact that \(|\psi_b^{\text{inv}}\rangle = V_b |\psi_b\rangle\) (Eq. (3.1)), we have

\[
P_{U}^{\text{max}} \geq \frac{1}{2} \max_{|\psi\rangle} \sum_{b \in \{0,1\}} \max_{U_b} |\langle \psi_b | (U_b \otimes I) | \psi \rangle|^2. \quad (3.9)
\]

We perform the maximization over \(|\psi\rangle\) for a given \(U_0\) and \(U_1\). By a variational approach, it is easy to show that the optimal \(|\psi\rangle\) has the form (up to an arbitrary overall phase)

\[
|\psi^{\text{max}}\rangle = \frac{|\tilde{\psi}_0\rangle + e^{-i \arg(\langle \tilde{\psi}_0 | \tilde{\psi}_1 \rangle)} |\tilde{\psi}_1\rangle}{\sqrt{2} \sqrt{1 + |\langle \tilde{\psi}_0 | \tilde{\psi}_1 \rangle|^2}}, \quad (3.10)
\]

where

\[
|\tilde{\psi}_0\rangle = (U_0 \otimes I) |\psi_0\rangle
\]

\[
|\tilde{\psi}_1\rangle = (U_1 \otimes I) |\psi_1\rangle.
\]

It follows that

\[
P_{U}^{\text{max}} \geq \frac{1}{2} \left( 1 + \max_{U_0, U_1} |\langle \psi_0 | U_0 U_1 \otimes I | \psi_1 \rangle| \right). \quad (3.11)
\]

Inequality (ii) now follows trivially from Uhlmann's theorem and the definition of Alice's control. \(\square\)

**Proof of Theorem 3.** Recall the definition of a purification BC protocol, provided in section 3.3. If Alice is honest she prepares the proof-token composite in either \(|\chi_0\rangle\) or
and submits the token system to Bob. In this case, the reduced density operators \( \rho_0 \) and \( \rho_1 \) that describe the token system are simply the trace over the proof system of \( |\chi_0\rangle \) and \( |\chi_1\rangle \), that is,
\[
\rho_b = \text{Tr}_p (|\chi_b\rangle \langle \chi_b|).
\]

The only cheating strategy available to Bob is to try to estimate the state of the token system, that is, to discriminate \( \rho_0 \) and \( \rho_1 \). It follows from state estimation theory that his maximum information gain is \( C^{\text{max}} = \frac{1}{2} D(\rho_0, \rho_1) \) and is achieved by performing a Helstrom measurement [40][41].

Alice can cheat in two ways in a purification BC protocol. She can cheat during the commitment phase by preparing the total system in a state \( |\psi\rangle \) that is different from \( |\chi_0\rangle \) or \( |\chi_1\rangle \), and she can cheat just prior to the unveiling phase by implementing a unitary operation \( U_b \) on the proof system. The identity of \( U_b \) can of course depend on which bit \( b \) she wishes to unveil.

Recalling that \( \Pi_b = |\chi_b\rangle \langle \chi_b| \), Alice's maximum probability of unveiling whatever bit she desires is
\[
P_{\text{U}}^{\text{max}} = \max_{|\psi\rangle} \sum_{b \in \{0,1\}} \frac{1}{2} \max_{U_b} |\langle \chi_b| U_b \otimes I |\psi\rangle|^2.
\]

Defining \( \rho \equiv \text{Tr}_p (|\psi\rangle \langle \psi|) \) and making use of Uhlmann's theorem, we obtain
\[
P_{\text{U}}^{\text{max}} = \frac{1}{2} \max_{\rho} \left( F(\rho, \rho_0)^2 + F(\rho, \rho_0)^2 \right).
\]

It now follows trivially from Lemma 2 and the definition of the control that \( C^{\text{max}} = \frac{1}{2} F(\rho_0, \rho_1) \). Alice achieves this control by implementing any unitary operations \( U_0 \) and \( U_1 \) that satisfy \( U_0 U_1 = U^{\text{max}} \) where \( U^{\text{max}} \) is defined in Eq. (3.8), and by initially preparing the state \( |\psi^{\text{max}}\rangle \) of Eq. (3.10) with \( |\psi_b\rangle = |\chi_b\rangle \). \( \square \)
3.6.2 Optimal trade-off relations

Given theorem 3, it is straightforward to determine the optimal trade-off relations between $G^{\max}$ and $C^{\max}$ for various restrictions on the states of Bob's system at the holding phase.

**Corollary 2** In Alice-supplied BC protocols where $\rho_0$ and $\rho_1$ are arbitrary, the optimal trade-off is

$$G^{\max} + C^{\max} = \frac{1}{2}$$

(This corresponds to curve II in Fig. 3.1).

**Proof.** This follows from theorem 3 and Eq. (3.3). \(\square\)

**Corollary 3** In Alice-supplied BC protocols where $\rho_0$ and $\rho_1$ either (1) have supports that lie in a single 2 dimensional Hilbert space, or (2) are not both mixed, the optimal trade-off is

$$G^{\max} + 2(C^{\max})^2 = \frac{1}{2}.$$  

(This corresponds to curve III in Fig. 3.1).

**Proof.** This follows from theorem 3, Eq. (3.6) and Lemma 1. \(\square\)

**Corollary 4** In Alice-supplied BC protocols where $\rho_0$ and $\rho_1$ are both pure states, the optimal trade-off is

$$\{G^{\max}\}^2 + \{C^{\max}\}^2 = \frac{1}{4}.$$  

(This corresponds to curve IV in Fig. 3.1).

**Proof.** This follows from theorem 3 and Eq. (3.5). \(\square\)

We now provide simple examples of protocols that achieve the optimal trade-offs of Corollaries 2-4.
To achieve the optimal trade-off of Corollary 2, it suffices to consider a purification BC protocol where \( \rho_0 \) and \( \rho_1 \) saturate the inequality of Eq. (3.3). The simplest example makes use of commuting density operators in a 3 dimensional Hilbert space. Specifically,

\[
\rho_0 = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \rho_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}.
\]

It is straightforward to show that \( D(\rho_0, \rho_1) = \lambda \) and \( F(\rho_0, \rho_1) = 1 - \lambda \), which implies that \( D(\rho_0, \rho_1) + F(\rho_0, \rho_1) = 1 \). It is worth emphasizing that a 3 dimensional Hilbert space is the smallest space in which this bound can be saturated, since states in a 2 dimensional Hilbert space must satisfy lemma 1.

We now provide a specific example of a family of protocols that achieve the optimal trade-off of Corollary 3. We consider purification BC protocols wherein

\[
\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \rho_1 = \begin{pmatrix} \lambda & 0 \\ 0 & 1-\lambda \end{pmatrix}.
\]

Note that this example qualifies both as an example where \( \rho_0 \) and \( \rho_1 \) have supports that lie in the same 2 dimensional Hilbert space, and as an example where one of \( \rho_0 \) and \( \rho_1 \) is pure. It is easy to see that \( D(\rho_0, \rho_1) = 1 - \lambda \) and \( F(\rho_0, \rho_1) = \sqrt{\lambda} \). Thus, we have saturated the lower bounds in Eq. (3.6) and lemma 1, and consequently, this family of protocols is optimal for the specified restrictions of \( \rho_0 \) and \( \rho_1 \).

It is trivial to find BC protocols that achieve the optimal trade-off of Corollary 4. Any purification BC protocol where \( \rho_0 \) and \( \rho_1 \) are pure states will do. Specifically, if

\[
\rho_0 = |0\rangle \langle 0| \quad \text{and} \quad \rho_1 = |\phi\rangle \langle \phi|,
\]
where $|\phi\rangle = \cos \phi |0\rangle + \sin \phi |1\rangle$, then one achieves every point on the curve $(C'_{\text{max}})^2 + (G'_{\text{max}})^2 = \frac{1}{4}$ by varying over all $\phi$ in the range 0 to $\pi/2$.

If we define a 'fair' BC protocol to be one where $C'_{\text{max}} = G'_{\text{max}}$, then by substituting this identity into the trade-off relations presented above, we obtain the following results. The best fair BC protocol from among the class of Alice-supplied BC protocols has $C'_{\text{max}} = G'_{\text{max}} = 0.25$ (point A on Fig. 3.1). The best fair BC protocol from among the class of Alice-supplied BC protocols where $\rho_0$ and $\rho_1$ are both qubit states or at least one of $\rho_0$ and $\rho_1$ is pure has $C'_{\text{max}} = G'_{\text{max}} = \frac{\sqrt{5} - 1}{4} \approx 0.30902$ (point B on Fig. 3.1). Finally, the best fair BC protocol from among the class of Alice-supplied BC protocols where $\rho_0$ and $\rho_1$ are both pure states has $C'_{\text{max}} = G'_{\text{max}} = \frac{1}{2\sqrt{2}} \approx 0.35355$ (point C on Fig. 3.1).

3.7 Significance for coin tossing

We briefly discuss the relevance of these results to coin tossing [14][17]. Coin tossing (CT) is a cryptographic task wherein at the end of the protocol both parties perform a measurement that has three outcomes corresponding to Alice winning, Bob winning, and the other party being caught cheating. If neither party is caught cheating, then the two measurements must agree on who won the coin toss. We can define a party's bias in a coin tossing protocol as the difference between their probability of winning and 1/2. A CT protocol with maximum bias $\alpha$ for Alice and maximum bias $\beta$ for Bob is one where if Bob is honest, the maximum Alice can make her probability of winning is $\frac{1}{2} + \alpha$, and if Alice is honest, the maximum Bob can make his probability of winning is $\frac{1}{2} + \beta$. Coin tossing can be built upon BC as follows. After the commitment phase, Bob sends Alice a bit which represents his guess of her commitment. If his guess corresponds to the bit Alice unveils, he wins the coin toss; if not, Alice wins. Our results show that it is possible to build a secure CT protocol for any pair of biases satisfying $\alpha + \beta \geq 1/2$, and that this inequality can be saturated. In particular, a fair CT protocol with both biases equal to
0.25 can be built up in this way. This last result has also been obtained by A. Ambainis using a generalized BB84 BC protocol [47].

Since CT is a weaker primitive than BC [15], the impossibility of a BC protocol that is arbitrarily concealing and binding does not imply the impossibility of a CT protocol with arbitrarily small biases for both parties [53]. Whether such a protocol is possible remains an open question in quantum cryptography.

It should be noted that even if such a CT protocol does not exist, the fact that there exist CT protocols with bounded biases for both parties is still potentially very useful. For instance, these can provide protocols for gambling [16] wherein both parties (the casino and the gambler) can be assured that their probability of winning is greater than some bound, regardless of the actions of the other party.

3.8 Conclusion

We have studied the extent to which BC protocols can be made simultaneously both partially concealing and partially binding. The degrees of concealment and bindingness were quantified by Bob's maximum information gain about the bit committed and Alice's maximum control over the bit she unveils. A lower bound on Alice's maximal control and Bob's maximum information gain for any BC protocol has been derived, although it is not known whether or not this bound can be saturated. A stronger lower bound was obtained for a restricted class of BC, called 'Alice-supplied' protocols, wherein Alice provides Bob with all of the systems that he makes use of during the commitment phase. Moreover, this lower bound has been shown to be saturated by what we have called a 'purification' BC protocol, wherein an honest Alice must prove her commitment to Bob by providing him with a purification of the state she submitted to him during the commitment phase.

Finally, we have considered the trade-off between concealment and bindingness for
Alice-supplied BC protocols given different constraints on $\rho_0$ and $\rho_1$ (these are the states of the systems in Bob's possession during the holding phase given commitments of 0 and 1 respectively). Such constraints might arise from practical restrictions on the physical implementation of a BC protocol. We have shown that for BC protocols where $\rho_0$ and $\rho_1$ have supports in a single 2D Hilbert space, or wherein $\rho_0$ and $\rho_1$ are not both mixed, one cannot achieve the optimal trade-off relation (that is, the optimal degree of bindingness for every degree of concealment). Using protocols wherein $\rho_0$ and $\rho_1$ are both pure, one does even worse. The optimal trade-off for Alice-supplied BC protocols is $C_{\text{max}} + G_{\text{max}} = \frac{1}{2}$ and can be achieved using a purification BC protocol wherein $\rho_0$ and $\rho_1$ are mixed but commuting states of a 3-dimensional Hilbert space.

The following question concerning the degrees of concealment and bindingness in BC protocols remains unanswered: do there exist any BC protocols with a trade-off relation that is better than the linear trade-off relation $C_{\text{max}} + G_{\text{max}} = \frac{1}{2}$? In order to settle this question, the scope of our analysis must be extended beyond Alice-supplied protocols. We conjecture that the linear trade-off is in fact the optimal trade-off from among all BC protocols.
Chapter 4

Spatial fragmentation of a Bose-Einstein condensate in a double-well potential

4.1 Introduction

The recent experimental demonstration of interference phenomena in Bose-condensed atomic gases [55], motivates a study of the spatial coherence of a condensate in a double-well potential. In particular, we are interested in the loss of spatial coherence that can occur at zero temperature due to fragmentation of the condensate. A fragmented condensate is one for which there is a macroscopic occupation of two or more orthogonal single-particle wavefunctions. If the occupied single-particle wavefunctions are spatially well separated, coherence over the spatial extent of the entire system will be lost, persisting only over the spatial extent of each fragment.

As Nozières [22] has pointed out, for repulsive inter-particle interactions it is the exchange energy that typically prevents fragmentation into a number of degenerate (or nearly degenerate) single-particle wavefunctions. However, this argument is inapplica-
ble for bosons in an external potential with several local minima, since single-particle wavefunctions that are localized about these minima may have very little overlap with one another, thereby leading to a very small exchange energy. Moreover, since the self-interaction energy in such a fragmented condensate is smaller than that of a single condensate, it is possible for the total interaction energy to be smaller as well. Although every particle in the fragmented condensate will pay a price in kinetic energy to occupy localized wavefunctions, the overall energy may still be less than that of a single condensate. Indeed, we show in appendix D that in the limit of a symmetric double-well potential with an infinitely strong central barrier, one can always find a fragmented state that has a total energy lower than any single condensate.

Thus we have the following situation in a double-well potential: in the absence of any central barrier the ground state is well approximated by a single condensate, while in the presence of an infinitely strong barrier it is well approximated by a fragmented condensate. It is clear therefore that there must be a transition between these two extremes as one increases the strength of the barrier. The first goal of this chapter is to propose a theoretical model for describing this transition. Specifically, we argue for an approximation of the fully interacting ground state that is more general than a Fock state, and that can be said to describe 'partial fragmentation' of the condensate. The equations that such a state must satisfy are derived within a variational approach. The second goal of the chapter is to solve these equations in a regime where the inter-particle interactions can be treated perturbatively. Numerical solutions of the equations and analytic approximations to these solutions are obtained within this regime. It should be noted that this limit is inappropriate for the description of the MIT condensate interference experiment [55], and consequently, our results do not specify the nature of the transition for this experimental set-up. Nonetheless, we expect the generic features of the transition to persist in the experimentally relevant regime.

We pause to consider previous treatments of this topic and their relation to this work.
Röhrle et al.[59] have provided a model of the MIT condensate interference experiment; however, it is a mean field analysis and therefore cannot describe fragmentation. Fragmentation in the case of attractive inter-particle interactions has been considered by Wilkin, Gunn and Smith [60], but this effect is qualitatively different from that of the repulsive case. Finally, Milburn et al. [57] have considered the energy eigenstates of a Bose-Einstein condensate in a double-well potential, and predict fragmentation when the inter-particle interactions are sufficiently strong. However, these authors consider only traps with weakly coupled wells, and therefore cannot determine the degree of fragmentation of the ground state in the regime of low barrier strengths where the coupling between the wells is strong. Moreover, this paper does not address the issue of the spatial coherence of the ground state. Since the presence of long-range order is a defining characteristic of Bose-Einstein condensation, it is critical to understand the manners in which this spatial coherence can be lost.

There has also been theoretical work on the problem of Bose condensates containing atoms in two different internal states, which is analogous to the two well problem. Esry et al. [61] determine the probability distributions and lifetimes of two interacting condensates in different internal states confined to the same trap, while Cirac et al. [62] as well as Steel and Collett [58] consider the ground states of such a system when the internal atomic states can be controlled by a Josephson-like laser coupling. In this case, the distinguishability of atoms in the two condensates is ensured by their internal state rather than their single-particle wavefunctions. However, the requirement of orthogonality in the spatial degrees of freedom is indispensable in a multiple well problem since it is precisely the shape of the single-particle wavefunctions that determines the degree of fragmentation in the system.

The remainder of the chapter is organized as follows. In section 4.2 we present our model and define some useful measures of spatial coherence of the condensate. In section 4.3 we present approximate analytic solutions of our model in the regime of nearly
non-interacting particles, and compare these to a numerical solution for a particular choice of the external potential. The experimental signature of fragmentation and finite temperature effects are discussed in section 4.5, followed by our concluding remarks in section 4.6.

4.2 The Model

4.2.1 The basic approach

Our system consists of an even number, $N$, of spinless bosons at zero temperature. We model the interactions by a two-particle pseudopotential in the shape-independent approximation, $V(r, r') = g\delta(r - r')$ with an interaction strength $g = 4\pi a_{sc} \hbar^2 / m$, where $a_{sc}$ is the s-wave scattering length, and $m$ is the mass of the bosons. The Hamiltonian is given by [63]

$$\hat{H} = \int d^3r \left[ -\frac{\hbar^2}{2m} \hat{\psi}^\dagger(r) \nabla^2 \hat{\psi}(r) + U(r) \hat{\psi}^\dagger(r) \hat{\psi}(r) + \frac{g}{2} \hat{\psi}^\dagger(r) \hat{\psi}^\dagger(r) \hat{\psi}(r) \hat{\psi}(r) \right]. \quad (4.1)$$

where $\hat{\psi}(r)$ is the quantum field operator, and $U(r)$ is the external potential. The external potential is taken to exhibit a single minimum along the $y$ and $z$ axes, and a double minimum along the $x$ axis. It is also taken to be symmetric about $x = 0$.

In order to capture the phenomenon of fragmentation in our model of the ground state, we must go beyond a mean field analysis. Specifically, we consider arbitrary superpositions of Fock states where up to two single-particle states are occupied. This corresponds to postulating a state vector of the form

$$|\psi\rangle = \sum_{N_1=0}^{N} C_{N_1} |N_1\rangle_{\phi_1} |N_2\rangle_{\phi_2}, \quad (4.2)$$
where

$$|N_1\rangle_{\phi_1} \langle N_2|_{\phi_2} = \frac{(a_1^\dagger)^{N_1} (a_2^\dagger)^{N_2}}{\sqrt{N_1} \sqrt{N_2}} |\text{vac}\rangle$$

is the Fock state in which $N_1$ particles occupy the single-particle state $\phi_1(r) = \langle r| a_1^\dagger |\text{vac}\rangle$ and $N_2$ particles occupy $\phi_2(r) = \langle r| a_2^\dagger |\text{vac}\rangle$. The total number of particles is fixed, $N_2 \equiv N - N_1$, the vector consisting of the set of coefficients $C_{N_1}$ is normalized, and the single-particle wavefunctions $\phi_1$ and $\phi_2$ are both normalized and orthogonal to one another.

The state (4.2) is certainly not the most general state one can consider. Indeed, a state such as (4.2) would be a poor choice if one were interested in studying the depletion of a single condensate due to interactions, since one there expects a certain fraction of the particles to be distributed among a macroscopic number of single-particle states. However, we are interested here in the possibility of the particles being redistributed into a few single-particle states that are each macroscopically occupied. We restrict ourselves to two single-particle states because the double-well geometry we are considering encourages fragmentation into two pieces [56]. Although it may be energetically favorable to fragment into more than two pieces at very high particle densities, we defer consideration of this possibility to a later work.

Among the many-body states defined by (4.2), we consider only those which have the same symmetry as the Hamiltonian under reflections about $x = 0$. This implies that the single-particle wavefunctions are mirror images of one another across $x = 0$ within a phase factor, $\phi_1(-x, y, z) = e^{i\theta} \phi_2(x, y, z)$, and that the coefficients satisfy $C_{N_1} = C_{N-N_1}$. With this assumption, and choosing $\phi_1$ and $\phi_2$ to be real, the Hamiltonian takes the form

$$\hat{H}_2 = \epsilon_{11} \hat{N} + \left(\epsilon_{12} + gT_1(\hat{N} - 1)\right) \left(a_1^\dagger a_2 + a_2^\dagger a_1\right)$$

$$+ \frac{gT_2}{2} \left(\hat{N}_1^2 + \hat{N}_2^2 - \hat{N}\right)$$

$$+ \frac{gT_2}{2} (a_1^\dagger a_1^\dagger a_2 a_2 + a_2^\dagger a_2^\dagger a_1 a_1 + 4\hat{N}_1 \hat{N}_2), \tag{4.3}$$
These quantities have the following physical interpretation: $\epsilon_{11}$ is the single-particle energy for the state $\phi_1$; $\epsilon_{12}$ is proportional to the inversion frequency of a single particle in the external potential; finally, $T_0$ quantifies the self-interaction energy, while $T_1$ and $T_2$ both quantify the cross-interaction energy.

In order to facilitate comparison of our work with earlier studies [57][58], we re-express the Hamiltonian in terms of operators satisfying angular momentum commutation relations, rather than in terms of the creation and annihilation operators we have employed thus far. We introduce the operators

$$
\hat{J}_z = \frac{1}{2}(a^\dagger_2 a_1 + a^\dagger_1 a_2),
\hat{J}_y = \frac{i}{2}(a^\dagger_1 a_2 - a_1^\dagger a_2),
\hat{J}_x = \frac{1}{2}(\hat{N}_2 - \hat{N}_1),
$$

which form an angular momentum algebra with total angular momentum $j = N/2$ [57]. In terms of these operators, the Hamiltonian can be rewritten as

$$
\hat{H}_2 = E_0 + 2(\epsilon_{12} + gT_1(N - 1)) \hat{J}_z + 2gT_2 \hat{J}_x^2 + g(T_0 - T_2) \hat{J}_x^2,
$$

(4.4)
where
\[ E_0 \equiv \epsilon_{11} N + \frac{1}{8} N(N + 2)(gT_0 + gT_2). \]
and where we have used \( \hat{J}_x^2 + \hat{J}_y^2 + \hat{J}_z^2 = j(j + 1) \) to eliminate \( \hat{J}_y^2 \) from the expression. The observable corresponding to \( \hat{J}_x \) is the particle number difference between the localized states \( \phi_1 \) and \( \phi_2 \). Defining the wavefunctions \( \phi_s = 2^{-1/2}(\phi_1 + \phi_2) \) and \( \phi_a = 2^{-1/2}(\phi_1 - \phi_2) \), which are respectively symmetric and antisymmetric about \( x = 0 \), one sees that \( \hat{J}_z \) can be rewritten as \( \frac{1}{2}(a_s^\dagger a_s - a_a^\dagger a_a) \), where \( a_s^\dagger \) and \( a_a^\dagger \) are the creation operators associated with \( \phi_s \) and \( \phi_a \) respectively. Thus, \( \hat{J}_z \) corresponds to the particle number difference between the symmetrized states \( \phi_s \) and \( \phi_a \). Finally, \( \hat{J}_y \) corresponds to the condensate momentum. Since we are considering the ground state it follows that \( \langle \hat{J}_y \rangle = 0 \), and since the ground state is symmetric under reflections about \( x = 0 \) it follows that \( \langle \hat{J}_x \rangle = 0 \).

### 4.2.2 A restricted variational principle

We now turn to the problem of identifying the ground state of our model. This can be achieved by minimizing the expectation value of \( \hat{H}_2 \) with respect to variations in both the coefficients \( C_{N_1} \) and the single-particle wavefunction \( \phi_1 \), subject to the constraints that the set of coefficients is normalized, and \( \phi_1 \) is both normalized and orthogonal to \( \phi_2 \), its mirror image about \( x = 0 \). However, it is in fact more convenient to minimize the expectation value of \( \hat{H}_2 \) with respect to variations in \( \phi_s \) and \( \phi_a \) rather than \( \phi_1 \). The reason for this is that no constraint corresponding to orthogonality is required when working with \( \phi_s \) and \( \phi_a \), since they are orthogonal by construction; as a result the analysis is simplified.

We begin with the variation of \( \phi_s \) and \( \phi_a \), implementing the normalization constraints through Lagrange multipliers \( E_s \) and \( E_a \) respectively. This results in two coupled non-linear Schrödinger equations for \( \phi_s \) and \( \phi_a \).
\[
\left[ \frac{-\hbar^2 \nabla^2}{2m} + U(r) + g \Gamma^o_\alpha \phi^2_\alpha(r) + g \Gamma^x_\alpha \phi^2_\beta(r) \right] \phi_\alpha(r) = E \phi_\alpha(r), \quad (4.5)
\]

where

\[
\begin{align*}
\Gamma^o_\alpha &= \left\langle (a^\dagger_\alpha a_\alpha)^2 - a^\dagger_\alpha a_\alpha \right\rangle / \left\langle a^\dagger_\alpha a_\alpha \right\rangle, \quad \text{and} \\
\Gamma^x_\alpha &= \left\langle a^\dagger_\alpha a^\dagger_\beta a_\beta + a^\dagger_\beta a^\dagger_\alpha a_\alpha + 4a^\dagger_\alpha a_\alpha a^\dagger_\beta a_\beta \right\rangle / \left\langle a^\dagger_\alpha a_\alpha \right\rangle.
\end{align*}
\]

and where the indices \((\alpha, \beta)\) take the values \((s, a)\) and \((a, s)\).

We now minimize the expectation value of \(\hat{H}_2\) with respect to variations in the \(C_{N_1}\), and implement the normalization constraint on the \(C_{N_1}\) through a Lagrange multiplier \(E\). This results in a five-term recurrence relation for the coefficients

\[
\begin{align*}
N \epsilon_{11} + \frac{g T_0}{2} \left( N_1^2 + N_2^2 - N \right) + 2g T_2 N_1 N_2 - E \right] C_{N_1} \\
+ \left[ \epsilon_{12} + g T_1 (N - 1) \right] \left[ \sqrt{N_1(N_2 + 1)} C_{N_1 - 1} + \sqrt{N_2(N_1 + 1)} C_{N_1 + 1} \right] \\
+ \frac{g T_2}{2} \left[ \sqrt{(N_1 - 1)N_1(N_2 + 1)(N_2 + 2)} C_{N_1 - 2} \\
+ \sqrt{(N_2 - 1)N_2(N_1 + 1)(N_1 + 2)} C_{N_1 + 2} \right] = 0, \quad (4.7)
\end{align*}
\]

for each value of \(N_1\); \(E\) is immediately identified as the expectation value of \(\hat{H}_2\). The latter set of equations forms a matrix eigenvalue equation for the \(N\)-element vector of coefficients \(C_{N_1}\). Given values for \(\epsilon_{11}, \epsilon_{12}, T_0, T_1\) and \(T_2\), we can solve this equation by diagonalizing an \(N \times N\) matrix with non-zero entries along five diagonals, a problem which is numerically tractable if the number of non-zero coefficients is not too large.

Since equations (4.5) and (4.7) form a coupled set of equations for \(\phi_s, \phi_a\) and the \(C_{N_1}\), we must in general solve these self-consistently. Of the many solutions thus obtained, the ground state is the one which minimizes the value of \(E\). However, it is not obvious that the solution that minimizes \(E_s\) and \(E_a\) also minimizes \(E\); thus it may be necessary to compare the energies of many solutions in order to find the ground state.
4.2.3 The regime of nearly non-interacting particles

The full problem outlined above is rather complex. We therefore consider only perturbative solutions of Eq. (4.5) in the nearly non-interacting regime, which we here define as the regime where the interaction energy is small compared to the difference between \( \epsilon_s^{(1)} \), the energy of the first symmetric excited state of the external potential, and \( \epsilon_s \), the energy of the ground state. This is ensured by the criterion

\[
gNT_0 \ll \epsilon_s^{(1)} - \epsilon_s. \tag{4.8}
\]

Since \( T_0 \) is on the order of the inverse of the volume of the trap, this criterion places an upper limit on the density of the condensate.

In this regime, we can treat the non-linear terms in (4.5) perturbatively. To obtain the expectation value of \( \hat{H}_2 \) to first order in the perturbation, we need only solve for the eigenfunctions of (4.5) to zeroth order. Thus, we need only solve the two linear Schrödinger equations

\[
\left[ -\frac{\hbar^2 \nabla^2}{2m} + U(r) - \epsilon_\alpha \right] \phi_\alpha(r) = 0, \tag{4.9}
\]

for \( \alpha = s, a \). In this case, the wavefunctions \( \phi_s \) and \( \phi_a \) are simply the two lowest single-particle energy eigenfunctions of the external potential, and the assumption of a state of the form of (4.2) corresponds to a two mode approximation.

The solutions of (4.9) determine the magnitudes of \( \epsilon_{11}, \epsilon_{12}, T_0, T_1 \) and \( T_2 \), and these subsequently define the form of the recurrence relation (4.7) that must be solved to obtain the coefficients \( C_{N_1} \). Although the full results are presented in section 4.3, it is illustrative to consider the ground state of \( \hat{H}_2 \) in two particularly simple limits: that of no barrier and that of an infinitely strong barrier.

In the absence of any barrier, \( |\epsilon_{12}| \simeq \epsilon_s^{(1)} - \epsilon_s \), and since \( |T_1| \) and \( T_2 \) are on the order of \( T_0 \) or less, it follows from the criterion (4.8) that \( |\epsilon_{12}| \gg NgT_0, Ng|T_1|, NgT_2 \). If
we provisionally assume that the ground state fulfils the conditions that \( N \left| \langle \hat{J}_z \rangle \right| \geq \langle \hat{j}_z^2 \rangle, \langle \hat{j}_z^2 \rangle \), then we are led to approximate the Hamiltonian by

\[
\hat{H}_2 \simeq E_0 + 2\epsilon_{12}\hat{J}_z. \tag{4.10}
\]

The ground state of (4.10) is simply the Fock state \( |N\rangle_{\phi_s} \) which describes \( N \) particles occupying the single-particle ground state \( \phi_s \). Since this solution satisfies our provisional assumption, the approximation is consistent. Such a Fock state is of course what one would expect for the ground state of a single well in the limit of nearly non-interacting particles. When this state is written in the form of (4.2), that is, in the basis of \( |N_1\rangle_{\phi_s}, |N_2\rangle_{\phi_s} \) states, rather than the basis of \( |N_s\rangle_{\phi_s} |N_a\rangle_{\phi_a} \) states, the coefficients \( C_{N_1} \) form a binomial distribution over \( N_1 \), centered at \( N/2 \). It seems appropriate to refer to any state of the form \( |N\rangle_{\phi_s} \) for macroscopic \( N \) and arbitrary \( \phi_0 \), as a ‘single condensate’. We are here only concerned with single condensates wherein the single-particle wavefunction \( \phi_0 \) is symmetric about \( x = 0 \). We do not introduce any additional terminology to distinguish such a state from one with arbitrary \( \phi_0 \), since no confusion is likely to arise.

In the limit of infinite barrier strength, the amplitudes of \( \phi_s \) and \( \phi_a \) at \( x = 0 \) are necessarily zero, while \( \phi_s \) and \( \phi_a \) at \( x \neq 0 \) satisfy the same equation. Consequently, \( \phi_s \) and \( \phi_a \) differ only in their symmetry under reflection about \( x = 0 \), and \( \epsilon_{12} = T_1 = T_2 = 0 \). The Hamiltonian of (4.4) then reduces to

\[
\hat{H}_2 = E_0 + gT_0\hat{J}_z^2. \tag{4.11}
\]

The ground state is \( |N/2\rangle_{\phi_1} |N/2\rangle_{\phi_2} \), which describes two independent condensates, or in other words, a condensate which is fragmented into two pieces. Since we are considering a potential well that is symmetric about \( x = 0 \), the two fragments are equally populated. It seems appropriate to refer to any state of the form \( |N_1\rangle_{\phi_1} |N_2\rangle_{\phi_2} \) where \( N_1 \) and \( N_2 \) are macroscopic and \( \phi_1 \) and \( \phi_2 \) are orthogonal, as a ‘dual condensate’ [64]. We will only be
concerned here with dual condensates wherein \( N_1 = N_2 = N/2 \), and \( \phi_1 \) and \( \phi_2 \) are mirror images of one another across \( x = 0 \).

The analysis above confirms, for the limit of nearly non-interacting particles, the results of an earlier study [56]: the ground state is well approximated by a single condensate at zero barrier strength, and a dual condensate at infinite barrier strength. At intermediate barrier strengths, we keep all the terms in \( \hat{H}_2 \) for our calculations. Although the cross-interaction terms are typically found to be small for generic shapes of the double-well potential, it is not obvious that these terms are negligible for an arbitrary potential, and thus we include them in our analytic results wherever possible.

### 4.2.4 Measures of the degree of fragmentation

Finally, in order to facilitate the interpretation of our results we highlight some observables that reveal the degree of spatial fragmentation of the condensate. The most useful observables for this purpose are those that probe the spatial coherence of the condensate across the barrier. In analogy to measures of optical coherence [65], we normalize the first-order correlation function, \( \rho_1(r, r') = \langle \hat{\Psi}^\dagger(r) \hat{\Psi}(r') \rangle \), to obtain the degree of first-order spatial coherence between points \( r \) and \( r' \),

\[
g^{(1)}(r, r') = \frac{\rho_1(r, r')}{[\rho_1(r, r)\rho_1(r', r')]^{1/2}}. \tag{4.12}
\]

Considering points \( r = (x, y, z) \) and \( r' = (-x, y, z) \) where \( x \) is positive and chosen to be sufficiently large so that \( |\phi_1(r)| \ll |\phi_2(r)| \) and \( |\phi_1(r')| \gg |\phi_2(r')| \), for any state of the form of 4.2 that is symmetric under reflection about \( x = 0 \), the quantity \( g^{(1)}(r, r') \) is in fact independent of \( r \) and \( r' \), and has the value

\[
C^{(1)} = \frac{\langle a_1^\dagger a_2 + a_2^\dagger a_1 \rangle}{N}. \tag{4.13}
\]
We refer to $C^{(1)}$ simply as the degree of first-order spatial coherence across the barrier. It is straightforward to verify that it attains its maximum value of 1 for a single condensate and a value of 0 for a dual condensate.

The second-order correlation function $\rho_2(r, r') = \left\langle \hat{\psi}^\dagger(r) \hat{\psi}^\dagger(r') \hat{\psi}(r) \hat{\psi}(r) \right\rangle$, which is simply the normally ordered density-density correlation, can be normalized to obtain the degree of second-order spatial coherence between points $r$ and $r'$,

$$g^{(2)}(r, r') = \frac{\rho_2(r, r')}{[\rho_2(r, r) \rho_2(r', r')]}^{1/2}.$$  \hspace{1cm} (4.14)

Defining $C^{(2)}$ in a manner completely analogous to $C^{(1)}$, we find

$$C^{(2)} = \frac{1 - 4\left(\frac{\Delta N_1}{N}\right)^2}{\frac{N-2}{2} + 4\left(\frac{\Delta N_1}{N}\right)^2},$$  \hspace{1cm} (4.15)

where $\Delta N_1 \equiv \left(\left\langle \hat{N}_1^2 \right\rangle - \left\langle \hat{N}_1 \right\rangle^2 \right)^{1/2}$ is the variance in the number of particles occupying the localized state $\phi_1$. We refer to $C^{(2)}$ as the degree of second-order spatial coherence across the barrier. The variance in $N_1$ for a single condensate $|N\rangle_{\phi_1}$ is that of a binomial distribution over $N_1$, namely $\sqrt{N}/2$. For a dual condensate the number of particles in a well is fixed, so that $\Delta N_1 = 0$. As a consequence, $C^{(2)} - 1 = 0$ for a single condensate $|N\rangle_{\phi_1}$, and $C^{(2)} - 1 = 2/N$ for a dual condensate. Since $\Delta N_1$ is sufficient to specify $C^{(2)}$, while being simpler to interpret, we use $\Delta N_1$ together with $C^{(1)}$ to characterize our results.

## 4.3 Analytic Approximations and Numerical Solutions

For a given shape of the double-well potential, it is straightforward to obtain the single particle ground state and first excited state by solving the linear Schrödinger equation...
(4.9). The localized single-particle states $\phi_1$ and $\phi_2$ are simply the sum and difference of the single-particle ground and first excited states. Using these wavefunctions, the coefficients $C_{N_1}$ can be obtained by solving the recurrence relation (4.7).

We here present approximate analytic solutions for the $C_{N_1}$ given an arbitrary shape of the double-well potential. Subsequently, we consider a particular form of the external potential for which the single particle ground and first excited states are obtained numerically. This allows us to obtain a numerical solution for the $C_{N_1}$ and to compare this solution to the analytic approximations.

4.3.1 Continuum approximation

Suppose the coefficients for the ground state satisfy the condition

$$|C_{N_1+1} - C_{N_1}| \ll C_{N_1}.$$

It is then useful to construct a function $C(u)$, defined over the real numbers, such that $C(u) = C_{N_1}$ at the discrete points $u = N^{-1}(N_1 - N/2)$, and such that $C'(u) \ll NC(u)$. Given this assumption of smoothness, a coefficient of the form $C_{N_1+p}$, where $p$ is a small integer, is well approximated by a Taylor expansion of $C(u + p/N)$ to second order in $p/N$. In this way, the recurrence relation (4.7) for the $C_{N_1}$ can be recast as a second order differential equation for the function $C(u)$. Moreover, any sum over $N_1$ can be approximated by an integral over $u$. In particular, the constraint of normalization for the coefficients is replaced by the constraint that the integral of $C^2(u)$ over all $u$ is $1/N$. The assumption of smoothness is readily verified to be appropriate for a single condensate, and we therefore expect it to continue to hold for solutions over a range of small barrier heights.

We also make use of the fact that the coefficients $C_{N_1}$ are significant only in the region where $N_1 \lesssim \sqrt{N}$, or equivalently, that the function $C(u)$ is significant only where
$u \ll \sqrt{1/N}$. This follows from the fact that any set of coefficients that has significant amplitude outside the range $N_1 \ll \sqrt{N}$ also has an energy that is larger than a single condensate; the interaction energy is greater since it scales with $\Delta N_1$, and the single-particle energy is greater since it is a minimum for a single condensate. It is therefore appropriate to expand each of the $N_1$-dependent terms as a power series in $u$:

$$\frac{2}{N} \sqrt{N_1(N_2 + 1)} = \sum_{n=0}^{\infty} I_n u^n,$$
$$\frac{4}{N^2} \sqrt{(N_1 - 1)N_1(N_2 + 1)(N_2 + 2)} = \sum_{n=0}^{\infty} J_n u^n,$$

which implicitly defines the $I_n$ and $J_n$.

The second-order differential equation for $C(u)$ we obtain is found to have a first-order term which can be eliminated by the substitution $\tilde{C}(u) = C(u) \exp(-\sum_n a_{2n} u^{2n})$ with an appropriate choice of the constants $a_{2n}$. It then follows that $\tilde{C}(u)$ satisfies a second-order differential equation identical to that of a particle with position $u$ in a one-dimensional potential well of even powers of $u$. Since the solution is only significant in the range $u \ll \sqrt{1/N}$, we make the approximation that terms in the potential that are quartic or of higher order in $u$ are small perturbations upon the quadratic term, and can be neglected. In this case, the function $\tilde{C}(u) = C(u) \exp(-\tau u^2/2)$ satisfies the equation for the modes of a simple harmonic oscillator:

$$-\tilde{C}''(u) + (\nu^2 + \tau^2)u^2 \tilde{C}(u) = (\eta + \tau)\tilde{C}(u),$$

where, after expanding the $I_n$ and $J_n$ to leading order in $1/N$,

$$\eta = \frac{2N^2 E/N - [\epsilon_{11} + \epsilon_{12} + Ng(\frac{1}{4} T_0 + T_1 + \frac{3}{4} T_2)]}{-\epsilon_{12} - Ng(T_1 + T_2)},$$
$$\nu^2 = \frac{2N^2}{-\epsilon_{12} - Ng(T_1 + T_2)} \left[ 2 \left( 1 - \frac{\eta}{N^2} \right) (-\epsilon_{12} - NgT_1) + Ng \left( T_0 + \left( 4 \frac{\eta}{N^2} - 3 \right) T_2 \right) \right],$$
$$\tau = 2. \quad (4.17)$$
Thus, the solution for $C(u)$ that minimizes $\eta$, thereby minimizing the energy $E$, is a Gaussian
\[
C(u) = \frac{1}{\sqrt{N}} \frac{1}{(2\pi)^{1/4}\sigma} e^{-\frac{u^2}{4\sigma^2}},
\]
(4.18)
with width
\[
\sigma = \frac{1}{2\sqrt{N}} \frac{1}{\sqrt{-A + \sqrt{A^2 + B}}},
\]
(4.19)
where
\[
A = \frac{3}{2N} \frac{-\epsilon_{12} - Ng(T_1 + \frac{4}{3}T_2)}{-\epsilon_{12} - Ng(T_1 + T_2)}, \quad \text{and}
\]
\[
B = \frac{-\epsilon_{12} - Ng(T_1 + \frac{3}{2}T_2 - \frac{1}{2}T_0)}{-\epsilon_{12} - Ng(T_1 + T_2)},
\]
and with energy
\[
E = N \left[\frac{-\epsilon_{12} - Ng(T_1 + T_2)}{4N^2\sigma^2} + (\epsilon_{11} + \epsilon_{12}) + Ng\left(\frac{1}{4}T_0 + T_1 + \frac{3}{4}T_2\right)\right].
\]
(4.20)
The variance in $N_1$ for this solution is simply $N\sigma$, while the degree of first-order spatial coherence is given by
\[
C^{(1)} = e^{-\frac{1}{2\sigma^2}} (1 + \frac{1}{N} - 2\sigma^2).
\]
(4.21)

In the absence of any barrier, $|\epsilon_{12}| \gg NgT_0, Ng|T_1|, NgT_2$, and it can be verified that Eq. (4.19) predicts the appropriate value for this limit, namely $\Delta N_1 \approx 1/2\sqrt{N}$, the value for a single condensate. As the barrier strength is increased, the magnitudes of $\epsilon_{12}, T_1$ and $T_2$ decrease while the magnitude of $T_0$ does not vary significantly; it therefore follows from (4.19) that $\Delta N_1$ will decrease with barrier strength. When $\Delta N_1$ falls below 1, the assumption of smoothness breaks down. Thus the range of validity of the continuum approximation is $\Delta N_1 \gtrsim 1$, or equivalently, $C^{(1)} \gtrsim 0.88$.

If the potential is such that $Ng|T_1|, NgT_2 \ll |\epsilon_{12}|$ continues to hold as the barrier strength is raised from zero, then to leading order in $1/N$ the expression for $\sigma$ simplifies
to

\[ \sigma = \frac{1}{2\sqrt{N}} \frac{1}{\sqrt{1 + \frac{N}{2} \frac{gT_0}{(-\epsilon_{12})}}} \]

depending only on the ratio of the interaction energy to the splitting between the symmetric and antisymmetric levels of the trap.

### 4.3.2 Two-coefficient approximation

At large barrier strengths, we make use of the following conditions:

\[ |\gamma| \ll 1, \quad \text{where} \quad \gamma \equiv \sqrt{\frac{N}{2}} \left( \frac{N}{2} + 1 \right) (-\epsilon_{12} - g(N - 1)T_1) \frac{gT_0}{gT_0} \]  \quad (4.22)

and

\[ |\zeta| \ll 1, \quad \text{where} \quad \zeta \equiv \frac{N^2gT_2}{\sqrt{\frac{N}{2}} \left( \frac{N}{2} + 1 \right) (-\epsilon_{12} - g(N - 1)T_1)} \]  \quad (4.23)

The first of these conditions is always satisfied for sufficiently strong barriers since in the limit of an infinitely strong barrier, \( \epsilon_{12} = T_1 = 0 \), while \( T_0 \) is finite. Moreover, we have numerically verified that the second condition holds at sufficiently large barrier strengths for a variety of external potentials. Within the domain of applicability of these conditions, we seek coefficients \( C_N \), that satisfy the recurrence relation (4.7) to first order in \( \gamma \) and \( \zeta \). Dividing the recurrence relation by \( gT_0 \), one finds that all terms involving \( N^2gT_2 \) have a magnitude on the order of \( \gamma\zeta \) and can therefore be neglected. In this limit, the following set of coefficients are a solution:
\[ C_{N_1} = \sqrt{1 - 2\gamma^2} \quad \text{for } N_1 = \frac{N}{2} \]
\[ = \gamma \quad \text{for } N_1 = \frac{N}{2} + 1, \frac{N}{2} - 1 \]
\[ = 0 \quad \text{otherwise.} \]  

(4.24)

The energy in this case is

\[ E = N\epsilon_{11} + \left( \frac{N(N-2)}{4} - 2\gamma^2 \right) gT_0. \]  

(4.25)

We refer to this approximation as the \textit{two-coefficient approximation}, and we dub any state of the form of (4.24) a \textit{perturbed dual condensate}. For such a state, \( C^{(1)} \) and \( \Delta N_1 \) are given by

\[ C^{(1)} = 2\gamma\sqrt{1 - 2\gamma^2}\sqrt{1 + \frac{2}{N}}, \quad \text{and} \]
\[ \Delta N_1 = \sqrt{2\gamma}. \]  

(4.26, 4.27)

Keeping terms to first order in \( \gamma \), and to leading order in powers of \( 1/N \), we have \( C^{(1)} = 2\gamma \). The range of validity of the two-coefficient approximation is the range of barrier strengths for which \( C^{(1)} \ll 1 \) and \( \Delta N_1 \ll 1 \).

An alternative manner of deriving this solution that is perhaps more physically intuitive, is to begin by assuming a state of the form of (4.24) and showing that the value of \( \gamma \) that minimizes the energy is indeed the value given in (4.22). We begin by recalling the form of \( \hat{H}_2 \), exhibited in (4.3). Assuming that \( |\zeta| \ll 1 \), the \( T_2 \) term in \( \hat{H}_2 \) can safely be neglected. If we introduce the operators

\[ \hat{n}_1 = \hat{N}_1 - \frac{N}{2}, \quad \text{and} \]
\[ \hat{n}_2 = \hat{N}_2 - \frac{N}{2}, \]
then we find that

\[
\langle \hat{H}_2 \rangle = E_{\text{dual}} + (\epsilon_{12} + gT_1 (N - 1)) \left( a_1^\dagger a_2 + a_2^\dagger a_1 \right) + \frac{1}{2} gT_0 (\langle \hat{n}_1^2 \rangle + \langle \hat{n}_2^2 \rangle),
\]

where \( E_{\text{dual}} \) is the energy of the dual condensate. Since the magnitude of the cross-interaction term involving \( T_1 \) only depends on the many-body state through expectation values of bilinear operators, this term together with the \( \epsilon_{12} \) term can be considered as an effective single-particle energy. To first order in \( \gamma \) and to leading order in \( 1/N \), the perturbed dual condensate has \( \left( a_1^\dagger a_2 + a_2^\dagger a_1 \right) = 2\gamma N \) and consequently it has an effective single-particle energy benefit over the dual condensate of \( 2\gamma N(-\epsilon_{12} - gNT_1) \) (this quantity is positive at the barrier strengths of interest, since \( \epsilon_{12} < 0 \) and typically \( T_1 < 0 \)). On the other hand, \( \langle \hat{n}_1^2 \rangle = \langle \hat{n}_2^2 \rangle = 2\gamma^2 \) for such a state, corresponding to a self-interaction energy cost of \( 2\gamma^2 gT_0 \). Thus, the effective single-particle energy of the perturbed dual condensate decreases linearly with \( \gamma \), while the self-interaction energy increases quadratically with this parameter. The minimum occurs precisely when \( \gamma \) has the value \( N(-\epsilon_{12} - gNT_1)/2gT_0 \), which approximates the value in (4.22) for \( N \gg 1 \).

For typical double-well potentials, where \( Ng |T_1| \ll |\epsilon_{12}| \), \( \gamma \) is well approximated by \( N(-\epsilon_{12})/2gT_0 \) to leading order in \( 1/N \). In this case, the transition from a completely fragmented condensate to one that shows some coherence across the barrier occurs when the number of particles times the ratio of the inversion frequency to the self-interaction energy becomes non-negligible. Thus, for a given shape of the trap and a fixed barrier strength, the degree of fragmentation decreases as the number of particles is increased but increases as the strength of the interaction is increased.
Figure 4.1: Numerical solutions for the single-particle wavefunctions $\phi_1(r)$ and $\phi_2(r)$ and the coefficients $C_{N_1}$ for $N = 100$ particles and double-well potentials with barrier strengths of $\alpha = 0, 15, 30, 45,$ and $60$ in units of $\sqrt{\hbar^2 \omega_x / m}$. The remaining parameter values are specified in the text. The dotted curve is the external potential along the $x$-axis, $U(x, y = 0, z = 0)$, in units of $\hbar \omega_x$. The solid and dashed curves are $\phi_1(x, y = 0, z = 0)$ and $\phi_2(x, y = 0, z = 0)$ respectively, in arbitrary units.
4.3.3 Numerical solutions

The form of the double-well potential in the MIT condensate interference experiment [55] is well modelled by a term that is harmonic along all three Cartesian axes, with frequencies $\omega_x$, $\omega_y$ and $\omega_z$ respectively, to which is added a Gaussian barrier of width $\delta$ and strength $\alpha$ centered at $x = 0$.

$$U(r) = m(\omega_x^2 x^2 + \omega_y^2 y^2 + \omega_z^2 z^2) + \frac{\alpha}{\sqrt{2\pi}\delta} e^{-\frac{x^2}{2\delta^2}}. \quad (4.28)$$

The parameter values appropriate for Ref. [55] are $\omega_x = 2\pi \times 19$ Hz, $\omega_y = \omega_z = 2\pi \times 250$ Hz, and $\delta = 6 \mu$m. Within such a trap, the criterion (4.8) for the applicability of our perturbative approach becomes $N \ll 100$, which is much smaller than the number of condensate atoms in their experiment. We consider instead a larger trap, specifically, one which is isotropic with the trapping frequency of the axis of weakest confinement in the MIT trap, $\omega_x = \omega_y = \omega_z = 2\pi \times 19$ Hz. In this case our perturbative approach is good for up to approximately $N = 100$ particles, and this is the example we consider.

The scattering length of $^{23}$Na is taken to be $a_{sc} = 3$ nm [66].

In Fig. 4.1 we plot the profile along the x-axis of the external potential $U(r)$ and the wavefunctions $\phi_1(r)$ and $\phi_2(r)$, together with the coefficients $C_{N_1}$ for several values of the barrier strength. Fig. 4.2 displays the degree of first order spatial coherence, $C^{(1)}$, and the variance, $\Delta N_1$, in the number of particles occupying the localized state $\phi_1$ as a function of the barrier strength. The generic features of these results persist for different choices of parameters in (4.28) as well as for different choices of the form of $U(r)$.

Also displayed in Fig. 4.2 are the values for $C^{(1)}$ and $\Delta N_1$ given by the continuum approximation, as specified by Eqs. (4.19) and (4.21), and given by the two-coefficient approximation, as specified by Eqs. (4.26) and (4.27), for the same choice of external potential. For their respective ranges of validity, the analytic approximations are found to fit the numerical results extremely well.
Figure 4.2: The degree of first-order spatial coherence across the barrier, $C^{(1)}$, and (b) the variance in the occupation number of one of the wells, $\Delta N_1$, as a function of the barrier strength, $\alpha$, in units of $\sqrt{\hbar^2 \omega_x / m}$ for $N = 100$ particles and the parameter values specified in the text. The solid curve is the numerical solution, the dashed curve is the continuum approximation, and the dotted curve is the two-coefficient approximation.
From these calculations arise the following picture of the transition between a single and a fragmented condensate. Moving up from zero barrier strength, there is a range of barrier strengths over which $C^{(1)}$ is close to unity, while $\Delta N_1$ falls from its single condensate value of $1/2\sqrt{N}$ to a value of 1. Moving down from infinite barrier strength, there is a range of barrier strengths over which $C^{(1)}$ and $\Delta N_1$ are both much less than 1. Between these two domains, there is a narrow range of barrier strengths wherein the greatest part of the transition in $C^{(1)}$ is made. The barrier strengths delimiting these domains can be estimated analytically using the approximations presented in this section.

4.4 Discussion

4.4.1 The experimental signature of fragmentation

Herein we consider a measurement of the first-order degree of spatial coherence. This is accomplished by a type of interference experiment that has been widely discussed in the literature [55][68][69][70][71]. Essentially, it constitutes a double-slit experiment for Bose condensates. The thought experiment runs as follows. After preparation of the condensate, the trap potential is removed and the atoms fall under the force of gravity through a pair of slits, located symmetrically about $x = 0$. These slits can be formed by changing the shape of the trapping potential, as long as this change is not so rapid that excitations are induced, and not so slow that the system has time to relax to a new many-body ground state. For simplicity of the analysis, we also assume that the particles on the left and right are each given momentum translations of magnitude $\hbar k$ towards one another [68]. In the absence of such translations, the interference pattern is simply more complicated, and has been studied by Röhl et al. [59]. We make the approximation that the inter-particle interactions are insignificant during this expansion period. In this case, only the single-particle wavefunctions evolve, while the coefficients $C_{N_1}$ in the many-body state (4.2) remain unchanged.
Suppose the slits are centered at points \( r = (x, y, z) \) and \( r' = (-x, y, z) \), where \( x \) is positive and chosen to be sufficiently large so that \( |\phi_1(r)| \ll |\phi_2(r)| \) and \( |\phi_1(r')| \gg |\phi_2(r')| \). In this case, the single-particle wavefunctions \( \phi_1(r) \) and \( \phi_2(r) \) evolve to wavefunctions localized entirely at just one of the slits. After the momentum translation and a period of free expansion the single-particle wavefunctions originating from the left and right of the barrier acquire complex phase factors of \( e^{ikz} \) and \( e^{-ikz} \) and magnitudes we denote by \( \tilde{\phi}_1(r) \) and \( \tilde{\phi}_2(r) \) respectively. For many-body states that are symmetric under a reflection about \( x = 0 \), these magnitudes are roughly uniform and of equal magnitude in the far field of the double-slit, so that the many-body state in the far field can be approximated by the many-body state prior to removal of the trap, with \( \phi_1(r) \) and \( \phi_2(r) \) replaced by \( e^{ikz} \) and \( e^{-ikz} \) respectively.

We now imagine detectors in the far field that are assumed to remove atoms from the condensate [69]. The probability distribution over the position, \( r_1 \), of the first detection is given by the expectation value of normally ordered field operators \( \hat{P}_1(r_1) = \frac{1}{N} \left\langle \hat{\Psi}_1^\dagger(r_1) \hat{\Psi}(r_1) \right\rangle \). The probability distribution over the positions \( r_1, r_2, ..., r_m \) of the first \( m \) detections is given by

\[
P^m(r_1, r_2, ..., r_m) = \frac{(N - m)!}{N!} \left\langle \hat{\Psi}_1^\dagger(r_1) \hat{\Psi}_1^\dagger(r_2) ... \hat{\Psi}_1^\dagger(r_m) \hat{\Psi}(r_1)...\hat{\Psi}(r_2) \hat{\Psi}(r_1) \right\rangle.
\]

The density of detection events that emerges in a single run of the double-slit experiment has the form \( \rho^m(r) = \frac{N}{m} \sum_{i=1}^{m} \delta(r - r_i) \) where the set of positions \( \{r_i\} \) are obtained from the probability distribution \( P^m(r_1, r_2, ..., r_m) \). Of course, the finite resolution of any realistic detector can be accounted for by replacing the delta function in this expression with a suitably broadened distribution; as long as the resolution is finer than the distance between the fringes of the interference pattern, the difference will not be significant.

In a single run of the double-slit experiment, both the single and dual condensates typically yield a distribution \( \rho^m(r) \) with essentially the maximum possible fringe visibility.
CHAPTER 4. SPATIAL FRAGMENTATION OF A BOSE-EINSTEIN CONDENSATE...

101

This is obviously true for a single condensate, and has been shown to be true for a dual condensate in the seminal paper of Javanainen and Yoo [69]. Thus, the mere presence of such interference is not indicative of a non-zero degree of first-order coherence. However, suppose the experiment is repeated many times with the same initial many-body state. In this case, the spatial phase of the interference pattern will vary randomly from one run to the next if the initial state is a dual condensate, while it will remain fixed if the initial state is a single condensate [69]. We therefore expect the degree of first-order spatial coherence to be revealed by the variance in the spatial phase of the interference pattern over many runs, or equivalently, the fringe visibility of the average detection pattern over many runs. Indeed, if one averages the pattern of detections from an infinite number of runs of the double-slit experiment, all prepared initially in the same many-body state, and each involving $m$ detection events, one obtains:

$$\bar{\rho}^m(r) = \int d^3r_1...d^3r_m\left(\frac{N}{m}\sum_{i=1}^{m} \delta(r - r_i)\right)P^m(r_1, r_2, ..., r_m)$$

$$= \frac{N}{m}\sum_{i=1}^{m} \int d^3r_1...d^3r_{i-1}d^3r_{i+1}...d^3r_mP^m(r_1, ..., r_{i-1}, r, r_{i+1}, ..., r_m)$$

$$= \left<\hat{\Psi}^\dagger(r)\hat{\Psi}(r)\right>. \quad (4.29)$$

The final equality follows from the fact that each element of the sum is simply equal to $P^1(r_i)$. If the fringe visibility of the average detection pattern, $\bar{\rho}^m(r)$, is evaluated for the many-body state in the far field, it is found to be precisely equal to our definition of $C^{(1)}$, the degree of first-order spatial coherence across the barrier, and thus enables a measurement of the latter.

Another possibility for an experimental study of fragmentation is a measurement of the degree of second-order spatial coherence; this may be accessible through non-resonant imaging [72].
4.4.2 Finite temperatures

We close this section with a few comments on the effect of finite temperatures on the coherence properties of the condensate. The excited states of the system are not in general well approximated by a state of the form of (4.2). Nonetheless it can be shown that at infinite barrier strength the first-order degree of spatial coherence across the barrier is zero for thermal equilibrium at any finite temperature. The proof is as follows. For an infinitely strong barrier the Hamiltonian is separable into two terms each involving only operators pertaining to particles on one side of the barrier. Consequently, any non-degenerate energy eigenstates are tensor products of states describing particles on one side of the barrier only. For any set of energy eigenstates that are degenerate, the subspace of Hilbert space spanned by this set has a basis of such product states. Thus, one can always identify a basis of energy eigenstates that are product states of this sort. Since the density operator that represents thermal equilibrium, \( \rho \), is a mixture of these energy eigenstates, we will necessarily have \( \text{Tr}(\rho \hat{\Psi}^\dagger(r) \hat{\Psi}(r')) = 0 \) if \( r \) and \( r' \) are on opposite sides of the barrier, and consequently the degree of first-order spatial coherence across the barrier for such a mixed state is zero as well. In the absence of any barrier, as long as the temperature is small enough that most of the particles are in the lowest single-particle energy level, the first-order degree of spatial coherence for the thermal state should be close to unity. For such temperatures, if the barrier strength is varied from zero to infinity, the first-order degree of spatial coherence of the thermal state will vary from nearly unity to zero. Thus, a significant transition must still occur at such temperatures.

4.5 Conclusions

A theoretical treatment of fragmentation in Bose condensates must go beyond a mean-field analysis. For the case of repulsive inter-particle interactions and a double-well
trapping potential, we have proposed an approach wherein an approximation to the many-body ground state is obtained by a restricted variational principle. We have implemented this proposal for the case of nearly non-interacting particles.

The coherence properties that we have considered are the degrees of first-order and second-order coherence across the central barrier of the potential. The first of these quantifies the variance over many runs in the spatial phase of the fringe pattern arising from the interference of atoms on either side of the barrier. The second is essentially the density-density correlation across the barrier, and for the states we consider it is a simple function of the variance in the number of particles in one of the wells. We find that as the barrier strength is increased, this variance is continuously squeezed down from its value for a single condensate. The degree of first-order spatial coherence is close to unity when this variance is greater than one, but thereafter drops off rapidly. Above a certain critical barrier strength we find that both quantities become much less than one, indicating that the condensate is essentially completely fragmented.

We have discussed how the degree of first-order coherence might be measured through interference experiments, and argued that a significant effect should be present even at finite temperatures. A concern, however, is that the ground state might be difficult to prepare if the relaxation time of the system is long compared to the lifetime of the condensate. This could arise if the only way for the particles to be redistributed across the barrier is by tunneling through it. However for numbers of particles that are not too large, this tunneling time need not be restrictive. For instance, in the example presented in Section 4.3.3, the single particle tunneling time at the barrier strength where $C^{(1)} = 0.88$ is approximately one minute, while at the barrier strength where $C^{(1)} = 0.1$ it is roughly one hour.

Our variational approach can be extended in a straightforward manner to the determination of the many-body ground state in systems where the external potential has an arbitrary number, $n$, of minima. In such cases, one would simply introduce states that are
arbitrary superpositions of Fock states where up to $n$ single-particle wavefunctions are occupied. Such an analysis should be of relevance to the determination of the coherence properties of Bose condensates in optical lattices. Moreover, at extremely high densities, where the interaction energy is dominant, it may become energetically favorable for a condensate to begin to fragment even in the presence of a perfectly uniform potential. We hope to address these possibilities in future work.
Chapter 5

A modal interpretation of quantum mechanics based on a principle of entropy minimization

5.1 Introduction

There are many reasons to seek a realist interpretation of quantum mechanics [25]. To date, however, no such attempt has gained widespread acceptance. One of the central problems of the realist program is to show that a quantum mechanical model of a microscopic system interacting with a macroscopic apparatus yields the same results as the standard operational description of the measurement process. Typically the difficulty lies in the interpretation of the total state vector when it cannot be written as a product state with respect to the system and apparatus, that is, when the two are entangled.

It has been suggested by many that what is lacking from quantum mechanics is an ‘interpretation basis’. Specifically, it is argued that there must be, at every moment in time, a basis of Hilbert space that is more physically significant than the others, and which is necessary to properly interpret the theory [74][75]. Rather than speaking of
a basis, one can equally well consider a \textit{decomposition} of the total state vector. To be precise, we define a decomposition of a vector \( |\psi\rangle \) as a set \( \{ (c_k, |\phi_k\rangle) \}_{k=1}^{m} \) of non-zero coefficients \( c_k \) and orthonormal vectors \( |\phi_k\rangle \) such that \( |\psi\rangle = \sum_{k=1}^{m} c_k |\phi_k\rangle \). We call the decomposition that is singled out as more physically relevant than the others at a given time the \textit{preferred decomposition}.

An appeal to a preferred decomposition can be made within the context of any of several different interpretive strategies. It has been suggested in the context of the many-worlds interpretation [74] as well as in the context of consistent histories [76]. It might also be useful in nonlinear modifications of quantum mechanics. However, the arena in which the concept of a preferred decomposition has been most discussed and has seen the most development is that of modal interpretations of quantum mechanics [32][33][25]. Modal interpretations are realist, no-collapse interpretations that assign values to variables according to certain constraints motivated by quantum logic. We have provided a review of the modal approach elsewhere [77]. The paper in question elaborates upon many of the fine points of this chapter, and as several references will be made to it, we refer to it here simply as SS.

There have been many proposals for the preferred decomposition within the modal approach. Bub and Clifton [78] have argued that Bohm's theory [79] can be formulated as a modal interpretation wherein the preferred decomposition contains only elements of the position basis\(^2\). Similarly, Bell's beable interpretation of quantum field theory [26] can be seen as a modal interpretation which uses the basis of eigenstates of local fermion number. In both these cases, the vector elements of the preferred decomposition are time independent. There also exist proposals wherein the vector elements of the preferred decomposition are explicitly time \textit{dependent}. Specifically, many authors have

\footnote{Note that the decompositions of vectors considered here should not be confused with the convex decompositions of density operators discussed in chapter 2.}

\footnote{Since, strictly speaking, the position and momentum operators are unbounded and have no eigenstates in the Hilbert space, this proposal must make use of the machinery of rigged Hilbert space. We do not consider such technicalities in this thesis.}
proposed using the bi-orthogonal (or Schmidt) decomposition as the preferred decomposition [34][35][36]. There have since been many proposals that are similar in kind. It has been suggested for instance that a particular tri-partite product decomposition, dubbed the tri-decomposition, should serve as the preferred decomposition in some circumstances [80]. This proposal has, however, been convincingly criticized [81]. More successful generalizations of this approach make use of decompositions with vector elements that are the tensor products of the elements of the spectral resolution of the density operators for each of the subsystems\(^3\). We call such decompositions *piece-wise spectral decompositions*, and we call approaches of this type *spectral modal interpretations*.

Spectral modal interpretations have received a great deal of attention in recent years. The two main examples of this approach are the version of the modal interpretation suggested by Vermaas and Dieks [37], which we shall refer to as the *VD proposal*, and the version of the modal interpretation suggested independently by Bacciagaluppi and Dickson [38] and by Dieks [39], which we shall refer to as the *BDD proposal*. These have several outstanding problems.

The VD proposal has Kochen-Specker type problems in the way it treats the relation between the properties of systems and the subsystems of which they are composed. As a no-go theorem due to Vermaas illustrates [86], it is impossible in the VD proposal to define a classical joint probability distribution for the properties of general collections of non-disjoint systems\(^4\). It has been proposed that a way out of this difficulty is to claim that a system receives properties only relative to a particular subdivision of the universe into disjoint systems. This view is called *perspectivalism*. We see the need for perspectivalism as the main problem of the VD proposal. However, even if one were willing to accept perspectivalism, the properties assigned to a system in the VD proposal

\(^3\)This constitutes an accurate description of the proposal only if there are no degeneracies in the piece-wise spectral decomposition. If there are degeneracies, then there are many piece-wise spectral decompositions, and one takes the intersection of the property ascriptions for all such decompositions.

\(^4\)By 'non-disjoint systems', we mean that the systems have some subsystem in common.
may depend sensitively on the form of the state vector, and this sensitive dependence threatens the solution of the measurement problem [91][83].

The BDD proposal was developed partly in response to the Kochen-Specker difficulties of the VD proposal. The critical new assumption in this approach is that there exists a distinguished division of the universe into elementary (atomic) subsystems, or equivalently, a distinguished factorization of the total Hilbert space, and that there are no properties of composites beyond those which are inherited from the atomic subsystems. Although this move avoids the Vermaas no-go theorem, it is at present unclear whether the BDD proposal succeeds in solving the quantum measurement problem. It can be shown that there will be instabilities in the property ascription to atomic systems [91], but whether such instabilities are consistent with stable properties of macroscopic systems has not yet been determined. More significantly, Vermaas' analysis of the BDD proposal [87] suggests to us that the properties assigned to apparatuses at the conclusion of measurements are unlikely to be consistent with our everyday perceptions of them for any realistic theoretical model of the measurement process.

Despite these problems, the spectral modal interpretations have a feature that we find quite appealing, namely that they can sometimes explain measurement results that are predictable with probability 1 as simply revealing the pre-existing value of the measured variable. We shall call the latter feature *faithfulness*. It is straightforward to show for instance that within the VD proposal faithfulness holds for very simple models of ideal measurements. It is likely that this was one of the early motivations for such an approach.

Faithfulness is only an empirical criterion in the context of measurements that are well described classically, where outcomes are perfectly predictable in principle and do reveal pre-existing properties. In general, however, a requirement of faithfulness is simply a requirement that the explanations of certain measurement outcomes have a particular form. Specifically, it is assumed that the reason a variable $V$ is found to have value $v$ in a measurement that is predictable with probability 1 is because immediately prior to the
measurement $V$ is determinate and has value $v$. Although this is perhaps the simplest form the explanation could take, it is not the only form, as is evidenced for instance by Bohm's theory [79] and Bell's be-able interpretation [26], where only the outcomes of measurements of certain variables (position in Bohm's case and lattice fermion number in Bell's case), are taken to reveal pre-existing values of these variables. The outcomes of measurements of other variables are explained in a different manner, for instance, by appeal to dispositional properties, collective effects or effective states [84].

Today there is less of an emphasis upon faithfulness. However, we read some authors as suggesting that this is the best explanation of perfectly predictable measurement results, and that it is to the detriment of a proposal if it must explain the results in some other way [87][85]. In any event, we feel that this feature is a useful motivation for a modal interpretation. For one, it yields a description of properties that is close to a standard view, namely, an interpretation which postulates collapses of the state vector whenever a measurement occurs. Secondly, whether there is any limit on the degree to which faithfulness can be satisfied is an interesting question in its own right.

In the spectral modal interpretations, faithfulness can be shown to fail for certain types of experiments. The results of Bacciagaluppi and Hemmo [85] imply that the VD proposal fails to exhibit faithfulness for experiments involving non-ideal measurements, in particular those that disturb the state of the system. One can easily verify that this argument also applies to the BDD proposal, although this should not be read as a failure of this proposal, since it never had faithfulness as a goal.

Our goal is to develop a modal interpretation that is more satisfactory with respect to the quantum measurement problem and with respect to faithfulness. We begin in section 5.2 with a novel proposal for the identity of the preferred decomposition of the state vector. Following previous authors [38][35], it is assumed that there is a distinguished factorization of the total Hilbert space. The preferred decomposition is singled out at every time as the one that minimizes a particular entropic quantity from among all
product decompositions with respect to the distinguished factorization. The minimum value of this entropy can be seen as a measure of the degree of entanglement of the state vector with respect to the distinguished factorization. We present the solution of the minimization problem for a class of state vectors.

Of course, merely providing a rule for determining the preferred decomposition at every time does not constitute an interpretation of quantum mechanics; there are many more features that must be specified. Bub and Clifton [78] have in fact developed a framework for modal interpretations wherein all features save the preferred decomposition are fixed. This framework is, however, not suitable for our purposes. First of all, the dynamics does not allow for time-dependent preferred decompositions. Given the work of Bacciagaluppi and Dickson [38] on dynamics for the Vermaas-Dieks version of the modal interpretation, the generalization of the Bub-Clifton framework is straightforward and has been provided in SS. Secondly, it was shown in SS that any modal interpretation that adopts certain restrictions on the form of the possible property ascriptions, of which Bub-Clifton is an example, cannot exhibit faithfulness for certain experiments involving disturbing measurements. A generalization of the Bub-Clifton framework that overcomes this difficulty was therefore developed in SS. In section 5.3, we present a review of this framework and make use of it to develop a modal interpretation based on our choice of the preferred decomposition.

In section 5.4, we discuss the circumstances under which the resulting proposal provides a solution to the measurement problem. It is found to be resolved for a large class of measurements given the standard model of the measurement process, as well as for more realistic extensions of these models. Finally, in section 5.5, we demonstrate that a large class of perfectly predictable measurements, including some that follow measurements which disturb the state of the system under investigation, exhibit faithfulness within the proposal. In section 5.6, we present our concluding remarks.
5.2 A preferred decomposition based on a principle of entropy minimization

We begin by introducing some terminology. A factorization $F$ of a Hilbert space $\mathcal{H}$ is defined to be a set of Hilbert spaces, each of dimensionality greater than one, the direct product of which is $\mathcal{H}$, that is, $F = \{ \mathcal{H}^{(p)} \}_{p=1}^{n}$, such that $\mathcal{H} = \mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)} \cdots \otimes \mathcal{H}^{(n)}$, and $\dim(\mathcal{H}^{(p)}) > 1$. A more precise definition of this concept is supplied by Bacciagaluppi [88], but this is not required for our purposes. A factorization containing $n$ elements is called $n$-partite, and the elements themselves are called factor spaces. A factorization $F$ is said to be a coarse-graining of a factorization $F'$, and $F'$ a fine-graining of $F$, if $F'$ can be generated from $F$ by factorizing one or more of the elements of $F$. A product decomposition of $|\psi\rangle$ with respect to the factorization $F = \{ \mathcal{H}^{(p)} \}_{p=1}^{n}$ is any decomposition $\{(c_k, \bigotimes_{p=1}^{n} |\phi_k^{(p)}\rangle)\}_{k=1}^{m}$ of $|\psi\rangle$ every element of which is a product state over $F$. Finally, an $n$-orthogonal decomposition is a product decomposition with respect to an $n$-partite factorization, the elements of which are orthogonal in every factor space, that is, a product decomposition for which $\{ |\phi_k^{(p)}\rangle \}_{k=1}^{m}$ is an orthogonal set for every value of $p$. If $n = 2$, such a decomposition is called bi-orthogonal.

The first element of the proposal is to assume that there is a factorization of the Hilbert space of the universe that is more physically relevant than the others: we call it the distinguished factorization. There is a precedent for such an assumption, specifically, in the modal interpretations of Healey [36], Bacciagaluppi and Dickson [38], and Dieks [39]. Some restrictions on the identity of the distinguished factorization will be discussed briefly in section 5.4.1.

The first constraint upon the preferred decomposition is that it be a product decomposition with respect to the distinguished factorization. This constraint is not sufficient to uniquely specify a decomposition. Indeed, the number of product decompositions of any state vector with respect to a given factorization is infinite. In order to distin-
guish between these, we turn our attention towards the coefficients in the decomposition. Since these coefficients define a probability distribution, different decompositions can be ordered with respect to the uniformity of the associated distributions. This uniformity can be quantified by several 'entropic' quantities. The most obvious candidate is the Shannon entropy, defined for a probability distribution $p = (p_1, p_2, ..., p_m)$ as

$$H(p) = -\sum_{k=1}^{m} p_k \log p_k.$$  \hspace{1cm} (5.1)

Thus, we can associate with every decomposition $D = \{(c_k, |\phi_k\rangle)\}_{k=1}^m$ of the state vector $|\psi\rangle$ the entropy

$$S_{|\psi\rangle}(D) = -\sum_{k=1}^{m} |c_k|^2 \log |c_k|^2.$$ \hspace{1cm} (5.2)

We refer to this quantity as the IU entropy of the state vector $|\psi\rangle$ for the decomposition $D$, since it has previously been considered by Ingarden and Urbanik [89], albeit in a very different context.

It is now possible to state our choice of preferred decomposition:

Given a distinguished factorization $F$, the preferred decomposition of the dynamical state vector $|\psi\rangle$ is the one that minimizes the IU entropy of $|\psi\rangle$ from among all product decompositions with respect to $F$.

By choosing the product decomposition that minimizes the IU entropy, we are choosing the interpretation where the probability distribution over the different possibilities is as narrow as possible. Moreover, since the minimum IU entropy (from among IU entropies for product decompositions) is zero if and only if $|\psi\rangle$ is a product state, it can be thought of as a measure of the entanglement of $|\psi\rangle$ with respect to the distinguished factorization. The strongest motivation for such a choice of preferred decomposition is that it appears very promising in securing a solution to the measurement problem and in satisfying the faithfulness criterion, as will be demonstrated in sections 5.4 and 5.5.
We do not however offer any \textit{a priori} justification of the principle.

Implementing the proposal requires solving the minimization problem for a given dynamical state vector and a given choice of distinguished factorization. If the distinguished factorization is bi-partite, the solution is given by the following theorem.

\textbf{Theorem 1} Suppose $|\psi\rangle$ is any vector in a Hilbert space with a bi-partite distinguished factorization $F_{bi}$. Any decomposition of $|\psi\rangle$ that is bi-orthogonal with respect to $F_{bi}$ minimizes the IU entropy from among all product decompositions of $|\psi\rangle$ with respect to $F_{bi}$.

The proof of this theorem is relegated to appendix E\textsuperscript{5}. In the case of an $n$-partite distinguished factorization, with $n > 2$, we have not yet found a solution to the minimization problem for all state vectors. However, the bi-partite result can be used to identify the preferred decomposition for some state vectors, as follows.

\textbf{Theorem 2} Suppose $|\psi\rangle$ is a vector in a Hilbert space with an $n$-partite distinguished factorization, $F_n$, where $n > 2$. If there exists a decomposition of $|\psi\rangle$ that is a product decomposition with respect to $F_n$ and that is a bi-orthogonal decomposition with respect to some bi-partite coarse-graining of $F_n$, then this decomposition minimizes the IU entropy from among all product decompositions with respect to $F_n$.

\textbf{Proof.} Suppose $F_{bi}$ is a bi-partite coarse-graining of $F_n$. The set $S_n$ of decompositions of $|\psi\rangle$ that are product decompositions with respect to $F_n$ is a subset of the set $S_{bi}$ that are product decompositions with respect to $F_{bi}$. We can denote this by $S_n \subseteq S_{bi}$. Moreover, suppose $D_n^{\min}(D_{bi}^{\min})$ is the decomposition that minimizes the IU entropy from among all the elements of $S_n(S_{bi})$. Theorem 1 shows that for every state vector $|\psi\rangle$, $D_{bi}^{\min}$ is the bi-orthogonal decomposition of $|\psi\rangle$. For certain state vectors, it may happen that $D_{bi}^{\min}$ lies

\textsuperscript{5}Although the formal proof is constructed for Hilbert space of finite dimension, we conjecture that it holds more generally.
among the elements of $S_n$. Since we know that $D_{bi}^{\text{min}}$ minimizes the IU entropy from among all the elements of $S_{bi}$, and $S_n \subseteq S_{bi}$, it follows that in this case $D_{bi}^{\text{min}}$ also minimizes the IU entropy from among all the elements of $S_n$. Thus, in this case $D_n^{\text{min}} = D_{bi}^{\text{min}}$. QED.

Theorem 2 is not a complete solution to the minimization problem because there exist state vectors for which $D_{bi}^{\text{min}}$ does not lie among the elements of $S_n$. Further work is required to determine the decomposition that minimizes the IU entropy in such cases.

We note that in the proof of theorem 1, presented in appendix E, the only relevant feature of the IU entropy is that it has the form $\sum_{k=1}^{n} f(|c_k|^2)$ for some concave function $f$. It follows that one would obtain the same results if, instead of minimizing the IU entropy, one minimized any other entropic quantity having this form. However, there is no guarantee that this insensitivity to the choice of entropic quantity persists in the more general case of state vectors for which theorem 2 does not apply.

A possible difficulty with the minimal entropy proposal as it stands has to do with the uniqueness of the preferred decomposition. It is well known that the bi-orthogonal decomposition of a state vector is not unique when the eigenvalues of the reduced density operator for one of the subsystems are degenerate. It follows from theorem 1 that if the distinguished factorization is bi-partite, then the decomposition that minimizes the IU entropy may not be unique, and the minimal entropy proposal may fail to uniquely specify a preferred decomposition. For instance, this occurs if the dynamical state vector is the EPR-Bell state for two spins $|\psi\rangle = 2^{-1/2}(|+a\rangle^{(1)} \otimes |-a\rangle^{(2)} - |a\rangle^{(1)} \otimes |a\rangle^{(2)}$). This difficulty persists in the case of an $n$-partite distinguished factorization, $F_n$, where $n > 2$, since, as can be shown using theorem 2, there are dynamical state vectors for which the decomposition that minimizes the IU entropy is non-unique, an example being a tensor product of EPR-Bell states. It should be noted, however, that in contrast to the bi-partite case a degeneracy among the eigenvalues of the reduced density operator for one of the factor spaces of $F_n$ does not necessarily imply a non-unique preferred decomposition. For instance, if the dynamical state vector has a decomposition that is
$n$-orthogonal with respect to the factorization $F_n$, then it follows from theorem 2 that this decomposition minimizes the IU entropy, and since the $n$-orthogonal decomposition is unique for $n > 2$ [90], so is the preferred decomposition. It is an open question whether the minimization of the IU entropy leads to a unique preferred decomposition when the dynamical state vector is such that theorem 2 does not apply.

It is useful to distinguish three types of non-uniqueness of the preferred decomposition: an instantaneous non-uniqueness, occurring at an isolated moment in time, an extended non-uniqueness, occurring over a finite interval of time, and a permanent non-uniqueness, which persists for all times.

It may be that the first type is not a serious problem. Suppose there is a way of associating elements of the preferred decomposition at different times so as to define paths through Hilbert space that are continuous functions of time. In fact, we have only been able to prove that the minimal entropy rule defines such a set of paths when theorem 2 applies continuously, since in this case the minimal entropy decomposition is a bi-orthogonal decomposition, which has been demonstrated to have continuous vector elements. Nonetheless, if such a set of paths can be defined in general, then the instantaneous non-uniqueness problem can be solved easily; the vector elements of the preferred decomposition at the moment of non-uniqueness are simply taken to be the limit of the paths defined at adjoining times. This is the same solution as was proposed in the context of the Vermaas-Dieks proposal [38][91].

If there do exist state vectors exhibiting an extended non-uniqueness, then this is a difficult problem for our proposal. However, it may be that a state vector undergoing Schrödinger evolution can only exhibit an instantaneous or a permanent non-uniqueness. An argument to this effect has been made for the occurrence of a non-unique bi-orthogonal decomposition [91]. This result can be applied to the minimal entropy proposal in cases where theorem 2 applies continuously, since in these cases, the minimal entropy decomposition is a bi-orthogonal decomposition. More generally, since the minimal entropy
decomposition is a generalization of the bi-orthogonal decomposition, it may be that a similar result also holds for the former. At present however this is merely speculation. It should also be noted that the argument cited above will fail if the state vector is not an analytic vector for the Hamiltonian operator, which might happen if the Hilbert space is infinite dimensional and the Hamiltonian is unbounded.

A permanent non-uniqueness in the preferred decomposition would also pose a challenge for the present proposal. One way in which such a non-uniqueness can arise is if the initial state of the universe happens by chance to be one that exhibits such non-uniqueness, and evolves under the Hamiltonian of the universe in such a way that this non-uniqueness persists over time. Assuming the initial state is selected at random from among all possible states, the probability of such a non-uniqueness depends on the measure of states in Hilbert space that exhibit permanent non-uniqueness. In instances where theorem 2 applies, a result of Bacciagaluppi, Donald and Vermaas shows that the set of states for which the preferred decomposition is non-unique is a set of measure zero. It is likely that a similar result will also hold in cases where theorem 2 does not apply.

Another way in which the dynamical state vector can exhibit non-uniqueness at all times is if there is some physical constraint, such as a symmetry principle, which enforces this non-uniqueness. Since in section 5.4.1 we argue that the distinguished factorization should also be fixed by symmetry principles, we speculate that the distinguished factorization might be chosen in such a way that a permanent non-uniqueness due to symmetry cannot arise. For instance, consider a universe consisting of two indistinguishable fermions. By the Pauli exclusion principle, the state vector for these particles would necessarily be anti-symmetrized at all times. If the distinguished factorization had a bi-partite coarse-graining $F_{hi}$, the elements of which described the degrees of freedom of each particle, and if theorem 2 applied, then by virtue of the degeneracy of the eigenvalues of the reduced density operator of either particle, the bi-orthogonal decomposition with respect to $F_{hi}$ would be permanently non-unique, and consequently so too would be the
minimal entropy decomposition. However, if the elements of the distinguished factorization were Hilbert spaces describing the occupation number of different field modes rather than Hilbert spaces describing the degrees of freedom of different particles, then this problem would not arise. Of course, at this stage we are considering interpretations of quantum field theory which is really beyond the scope of this investigation. Nonetheless, the example illustrates the point.

5.3 The minimal entropy proposal as a modal interpretation

In SS, we presented a framework for modal interpretations of quantum mechanics which was a generalization of the one proposed by Bub and Clifton [78]. We briefly recall the structure of this generalized framework here.

We consider the universe as a closed system described by a state vector obeying the Schrödinger equation. We call this vector the dynamical state vector, and denote it by $|\psi(t)\rangle$. At every time, the interpretation must specify a preferred decomposition of the dynamical state vector. Moreover, at every time, a single vector element from among the elements in the preferred decomposition is singled out as fixing the properties of the universe; we call it the property state vector, and denote it by $|\Phi(t)\rangle$. The properties of the universe are fixed as follows. Variables that are associated with Hermitian operators in the total Hilbert space that have the property state vector as an eigenstate receive a value, namely, the associated eigenvalue. These variables are called determinate. Variables that do not have the property state vector as an eigenstate do not receive any value and are said to be indeterminate. We refer to the set of determinate variables for the universe together with the value assignment to its members as the property ascription for the universe.

If $\mathcal{DV}$ denotes the set of determinate variables, and $[V]$ denotes the value of a variable
$V$, then the property ascription at a given time $t$ can be summarized as follows:

$$
\mathcal{D}V = \{ V | V | \Phi(t) \rangle \propto | \Phi(t) \rangle \},
$$

$$
[V] = \langle \Phi(t) | V | \Phi(t) \rangle.
$$

Thus far we have considered only the property assignment to the universe as a whole. We now turn to subsystems. Again, we refer to the set of determinate variables for the system together with the value assignment to its members as the *property ascription* for the system. Variables that are associated with Hermitian operators that act on a subspace, $\mathcal{H}^A$, of the total Hilbert space, $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^{\bar{A}}$, are assigned values in accordance with the *reductionist rule*:

$$
V^A \in \mathcal{D}V^A \text{ if and only if } V^A \otimes I^{\bar{A}} \in \mathcal{D}V, \text{ and } [V^A] = [V^A \otimes I^{\bar{A}}],
$$

where $\mathcal{D}V^A$ is the set of determinate variables for the system $A$, $\mathcal{D}V$ is the set of determinate variables for the total system, and $I^{\bar{A}}$ denotes the identity operator for system $\bar{A}$.

The only constraint that is placed upon the choice of preferred decomposition (at least at the stage of simply defining the framework), is that the vector elements of the preferred decomposition must be differentiable functions of time$^6$. This is called the *constraint of differentiability*. Given this constraint, these elements, which we denote by $\{ | \phi_k(t) \rangle \}_{k=1}^4$, will obey a time-dependent Schrödinger equation

$$
\frac{d}{dt} | \phi_k(t) \rangle = -i \tilde{H}(t) | \phi_k(t) \rangle,
$$

$^6$Technicities concerning the possibility of the cardinality of the preferred decomposition changing over time are discussed in SS.
for some Hermitian operator $\tilde{H}(t)$. The set of paths through Hilbert space that the elements of the preferred decomposition define are called the preferred paths.

Finally, the framework also specifies the possible forms for the dynamics. The property state vector is taken to undergo a stochastic Markovian dynamics among the preferred paths, where the probability $p_k(t)dt$ of being on the $k$th path in the interval $[t, t+dt]$ is simply

$$p_k(t) = |\langle \phi_k(t)|\psi(t)\rangle|^2 . \quad (5.6)$$

Following previous work [26][92][38], summarized in SS, it can be shown that the most general form of Markovian dynamics satisfying Eq. (5.6) is the following. If $T_{kj}(t)dt$ denotes the probability of a transition from preferred path $j$ to $k$ in the interval $[t, t+dt]$, then we require that

$$T_{kj}(t) \geq \max\{0, \frac{J_{kj}(t)}{p_j(t)}\} , \quad (5.7)$$

and

$$T_{jk}(t) = \frac{(T_{kj}(t)p_j(t) - J_{kj}(t))}{p_k(t)} . \quad (5.8a)$$

for every pair of indices $k > j$, where the set of currents $J_{kj}(t)$ must satisfy

$$\sum_j J_{kj}(t) = 2 \text{Im} \left[ \langle \psi(t)|\phi_k(t)\rangle \langle \phi_k(t)|H - \tilde{H}(t)|\psi(t)\rangle \right] . \quad (5.9)$$

There are an infinite number of choices of $J_{kj}(t)$ and $T_{kj}(t)$ that satisfy these equations.

So we see that there are two features left unspecified by the framework: (1) the identity of the preferred decomposition, and (2) the explicit form of the dynamics.

In this investigation, we wish to consider the consequences of adopting as preferred the decomposition discussed in section 5.2, namely, the decomposition that minimizes the IU entropy from among all product decompositions with respect to the distinguished factorization. Given theorem 2, it is possible to show that this decomposition, when considered as a function of time, satisfies the constraint of differentiability in some cases. In
particular, if the dynamical state vector evolves in such a way that it has a bi-orthogonal decomposition with respect to some coarse-graining of the distinguished factorization for a finite interval of time, then Eq. (5.5) can be satisfied for that interval. The reason is that the vector elements of a bi-orthogonal decomposition are analytic functions of time [38]. This result is not very useful, however, since we will argue in section 5.5 that theorem 2 is unlikely to hold over a finite interval of time for certain kinds of interacting systems. Indeed, this fact is critical in ensuring that the minimal entropy proposal does not suffer from the same instability problems that arise in the Vermaas Dieks proposal. It remains an open problem whether for arbitrary dynamical state vectors the decomposition that minimizes the IU entropy, considered as a function of time, satisfies the differentiability constraint. If this is indeed the case, then the entropy minimization rule defines a set of preferred paths.

Although the dynamics of the property state vector is not the focus of the present investigation, we make an explicit choice of dynamics in order to complete the proposal. We follow Bacciagaluppi and Dickson [38] in adopting what they have called the 

*generalized Schrödinger dynamics:*

\[ J_{kj}(t) = 2 \text{Im} \left[ \langle \psi(t)|\phi_k(t) \rangle \langle \phi_k(t)|H - \tilde{H}(t)|\phi_j(t) \rangle \langle \phi_j(t)|\psi(t) \rangle \right], \quad (5.10) \]

and

\[ T_{kj}(t) = \max\{0, \frac{J_{kj}(t)}{p_j(t)} \}. \quad (5.11) \]

This is a generalization to time-dependent preferred decompositions of the choice made by Bell [26], Vink [92] and Bub [25]. Since the inequality in Eq. (5.7) is saturated, this choice of \( T_{kj}(t) \) minimizes the degree of stochasticity for a given form of the current. Such a choice is motivated primarily by its simplicity.

For convenience, we refer to the modal interpretation that results from these choices of preferred decomposition and dynamics as the 

*minimal entropy proposal.*
It is worth emphasizing some of the novel features of the property ascription in the minimal entropy proposal. Since the preferred decomposition is always a product decomposition with respect to the distinguished factorization $F = \{ \mathcal{H}^{(p)} \}_{p=1}^{n}$, the property state vector can always be written as a product state with respect to this factorization

$$|\Phi(t)\rangle = \bigotimes_{p=1}^{n} |\phi^{(p)}(t)\rangle.$$

It then follows from the definition of the property ascription for the universe, specified in Eq. (5.3) and the reductionist rule, specified in Eq. (5.4), that the property ascription for the $p$th subsystem is simply given by

$$D V^{(p)} = \{ V^{(p)} | V^{(p)} \phi^{(p)}(t) \rangle \propto | \phi^{(p)}(t) \rangle \},$$

$$[ V^{(p)} ] = \langle \phi^{(p)}(t) | V^{(p)} | \phi^{(p)}(t) \rangle.$$

Although this is of the same form as Eq. (5.3), there remains a significant difference between the possible property ascriptions for the universe and a subsystem thereof. The different possibilities for the identity of the property state vector $|\Phi(t)\rangle$ at a given time form an orthonormal set of vectors (since the preferred decomposition was assumed to consist of orthogonal vectors), while the different possibilities for the identity of the vector $| \phi^{(p)}(t) \rangle$ for a given value of $p$ at a given time do not necessarily form an orthogonal set. This non-orthogonality for the distinguished subsystems is critical to ensuring that the faithfulness criterion can be satisfied for experiments involving disturbing measurements upon these systems, as is discussed in section 5.5.

### 5.4 The quantum measurement problem

We now consider the extent to which the minimal entropy proposal solves the quantum measurement problem. Although this term is often taken to refer to the whole cluster of
conceptual difficulties surrounding measurement, we shall use it to refer to the particular problem of deriving operational quantum mechanics from a realist, no-collapse interpretation. To consider the problem, we must introduce a quantum mechanical model of the measurement procedure, that is, a model of the interaction between the degrees of freedom of the system under investigation, the apparatus, and the environment. We discuss both single measurements and sequences of measurements.

5.4.1 Single measurements

Standard models of measurement

We consider the measurement associated with a Hermitian operator $V$, acting over a Hilbert space $\mathcal{H}^S$, the eigenvalues of which are non-degenerate and the eigenvectors of which are denoted by $\{ |\varphi_k\rangle \}_{k=1}^n$. Assuming the preparation procedure is associated with a vector $\sum_k c_k |\varphi_k\rangle$, where $\sum_k |c_k|^2 = 1$, operational quantum mechanics predicts, via the Born rule, that the measurement will have outcome $k$ with probability $|c_k|^2$.

We now consider a quantum mechanical model of the measurement process. The system under investigation is called the object system. This is made to interact with a macroscopic apparatus, associated with a Hilbert space $\mathcal{H}^A$, which in turn interacts with a macroscopic environment, associated with a Hilbert space $\mathcal{H}^E$. Given an initial state vector in $\mathcal{H}^S \otimes \mathcal{H}^A \otimes \mathcal{H}^E$, one could in principle determine the evolution of the total system using the full microscopic Hamiltonian.

In practice of course the problem is far too complex to be solved exactly. Nonetheless, there is a set of standard toy models of measurement that are commonly used to investigate realist interpretations. These models adopt some simplifying assumptions about the initial state and the form of the evolution. Specifically, it is assumed that the object system, apparatus and environment are all initially uncorrelated, so that the initial dynamical state vector has the form $|\varphi_k\rangle \otimes |A_0\rangle \otimes |E_0\rangle$, a product state with respect to the
factorization \( \{ \mathcal{H}^S, \mathcal{H}^A, \mathcal{H}^E \} \) of the Hilbert space. The dynamics is assumed to be such that

\[
|\varphi_k \rangle \otimes |A_0 \rangle \otimes |E_0 \rangle \mapsto |\tilde{\varphi}_k \rangle \otimes |A_k \rangle \otimes |E_k \rangle ,
\]

(5.12)

where \( \{|A_k\rangle\}_{k=1}^m \) is a set of orthonormal vectors for the apparatus, \( \{|E_k\rangle\}_{k=1}^m \) is a set of orthonormal vectors for the environment, and \( \{|\tilde{\varphi}_k\rangle\}_{k=1}^m \) is a set of normalized but possibly non-orthogonal vectors for the object system, and where '\( \mapsto \) ' denotes the mapping corresponding to the unitary evolution.

The property associated with the projector \( P_{A_k} \equiv |A_k \rangle \langle A_k | \) must be such that the apparatus can be accurately described as 'indicating outcome \( k \)'. For instance, if the apparatus indicates the outcome by a digital display, \( P_{A_k} \) must correspond to the property of displaying the number \( k \). Similarly, the property associated with the projector \( P_{A_0} \equiv |A_0 \rangle \langle A_0 | \) must be such that the apparatus can be accurately described as 'ready to measure'.

If the initial vector for the object system is \( \sum_k c_k |\varphi_k \rangle \), the final dynamical state vector for the total system, given Eq. (5.12) and the assumption that the evolution is linear, is

\[
|\psi_{\text{final}} \rangle = \sum_{k=1}^m c_k |\tilde{\varphi}_k \rangle \otimes |A_k \rangle \otimes |E_k \rangle .
\]

(5.13)

We are now in a position to ask whether a given realist no-collapse interpretation falls prey to the quantum measurement problem within this model. We begin by illustrating the problem in the traditional manner, specifically, in the context of the simplest realist no-collapse interpretation one can imagine: one where the reductionist rule holds, and a variable is determinate if and only if it has the dynamical state vector as an eigenstate, in which case its value is the corresponding eigenvalue. Such an interpretation has been called the 'bare theory' by Albert [93]. Within the framework presented in section 5.3, it corresponds to adopting the trivial decomposition of the dynamical state vector as
Consider first a case where \( c_k \neq 0 \) for only a single value of \( k \), that is, where the initial state vector of the object system is an eigenstate of \( V \). The final state vector is then of the form \( |\tilde{\psi}_k\rangle \otimes |A_k\rangle \otimes |E_k\rangle \). Within the bare theory, the projector \( P_{A_k} \equiv |A_k\rangle \langle A_k| \) for the apparatus is determinate and receives the value 1. Thus, the apparatus can be accurately described as 'indicating outcome \( k \).

If, on the other hand, the initial state is such that \( c_k \neq 0 \) for more than one value of \( k \), then the final state vector is of the form \( \sum_k' c_k |\tilde{\psi}_k\rangle \otimes |A_k\rangle \otimes |E_k\rangle \), where \( \sum_k' \) indicates a sum over values of \( k \) for which \( c_k \neq 0 \). In this case, the projector \( \sum_k' P_{A_k} \) for the apparatus is determinate and receives the value 1, while no projector of the form \( P_{A_k} \) is determinate or receives the value 1 for any value of \( k \). Thus, the bare theory does not predict that the apparatus indicates the outcome \( k \) for any value of \( k \) for which \( c_k \neq 0 \). Hence the bare theory does not reproduce the predictions of operational quantum mechanics. This is the quantum measurement problem.

We now specify the assumptions under which the minimal entropy proposal solves this problem. These involve the nature of the distinguished factorization, which we have not yet specified. Whatever it might be, the distinguished factorization should be defined in terms of primitives of the theory and selected by physical principles, for instance, from considerations of symmetry. We do not here take a stand on the identity of the distinguished factorization; a discussion of the issue can be found in Dieks [39], wherein it is argued that a necessary condition on this choice is that the factor spaces carry an irreducible representation of the space-time group (the Galilei group in nonrelativistic quantum mechanics). For the present, we insist only that the distinguished factorization, which we denote by \( F \), has the factorization \( \{H^S, H^A, H^E\} \) as a coarse-graining, and that its elements correspond to microscopic degrees of freedom. For instance, they could correspond to degrees of freedom of elementary particles.

Now, suppose that \( F \) is such that all the vectors in the sets \( \{ |\tilde{\psi}_k\rangle \}_{k=1}^m \), \( \{ |A_k\rangle \}_{k=1}^m \).
and \(\{|E_k\rangle\}_{k=1}^{n}\) are product states with respect to it. One can then determine that the preferred decomposition of \(|\psi_{\text{final}}\rangle\) is

\[
D_{\text{final}} = \{(c_k, |\tilde{\varphi}_k\rangle \otimes |A_k\rangle \otimes |E_k\rangle)\}_{k=1}^{n}.
\]

This follows from theorem 2 and the fact that \(D_{\text{final}}\) is a product decomposition with respect to \(F\) that is bi-orthogonal with respect to \(F_{\text{bi}} = \{\mathcal{H}^S \otimes \mathcal{H}^A, \mathcal{H}^E\}\), which is a coarse-graining of \(F\). It then follows from Eq. (5.6) that, with probability \(|c_k|^2\), the property state vector is

\[
|\Phi_{\text{final}}\rangle = |\tilde{\varphi}_k\rangle \otimes |A_k\rangle \otimes |E_k\rangle.
\]

Using the reductionist rule we find that the projector \(P_{A_k}\) is determinate and receives the value 1 with probability \(|c_k|^2\). Thus the apparatus has the property of indicating outcome \(k\) with probability \(|c_k|^2\). This is in agreement with the predictions of operational quantum mechanics.

Thus, we have obtained a solution to the measurement problem within the standard model of measurement. In so doing, we have assumed that when the initial state vector of the object system is an eigenstate of \(V\), the final dynamical state vector for the total system is unentangled with respect to the distinguished factorization.

The assumption of no entanglement between the distinguished factor spaces of the apparatus and the environment is not particularly realistic, given that these factor spaces are taken to correspond to microscopic degrees of freedom, and typical interactions between the apparatus and the environment are likely to entangle these degrees of freedom. However, this assumption can be relaxed somewhat without changing any of our conclusions, as we now demonstrate.

We consider a model of measurement wherein the evolution is of the form:

\[
|\varphi_k\rangle \otimes |A_0\rangle \otimes |E_0\rangle \mapsto |\tilde{\varphi}_k\rangle \otimes \sum_{\mu=1}^{M} f_{k,\mu} (|A_{k,\mu}\rangle \otimes |E_{k,\mu}\rangle).
\]  (5.14)
where $\sum_{\mu} |f_{k,\mu}|^2 = 1$ and where $\{|\tilde{\phi}_k\rangle\}_{k=1}^m$, $\{|A_{k,\mu}\rangle\}_{\mu=1}^M$, and $\{|E_{k,\mu}\rangle\}_{\mu=1}^M$ are orthonormal sets of vectors that are product states with respect to $F$. For every value of $\mu$, the property associated with the projector $P_{A_{k,\mu}} \equiv |A_{k,\mu}\rangle \langle A_{k,\mu}|$ must be such that the apparatus can be accurately described as 'indicating outcome $k$'. That there can be more than one projector corresponding to indicating a particular outcome is not unreasonable since there can be many different microscopic configurations of the apparatus leading to the same overall macroscopic appearance.

An arbitrary initial state vector for the object system, $\sum_k c_k |\varphi_k\rangle$, leads, via Eq. (5.14), to the following final dynamical state vector for the total system:

$$|\psi_{\text{final}}\rangle = \sum_{k=1}^m c_k |\tilde{\phi}_k\rangle \otimes \sum_{\mu=1}^M f_{k,\mu} (|A_{k,\mu}\rangle \otimes |E_{k,\mu}\rangle).$$

The preferred decomposition of this state vector is

$$D'_{\text{final}} = \left\{ (c_k f_{k,\mu}, |\tilde{\phi}_k\rangle \otimes |A_{k,\mu}\rangle \otimes |E_{k,\mu}\rangle) \right\}_{\mu=1}^M,$$

since this is a product decomposition with respect to $F$ that is bi-orthogonal with respect to $F_{\text{bi}}$. It follows that the property state vector is

$$|\Phi'_{\text{final}}\rangle = |\tilde{\phi}_k\rangle \otimes |A_{k,\mu}\rangle \otimes |E_{k,\mu}\rangle$$

with probability $|c_k f_{k,\mu}|^2$. By the reductionist rule, the projector $P_{A_{k,\mu}}$ is determinate and receives value 1 with probability $|c_k f_{k,\mu}|^2$. Thus the apparatus has the property of indicating outcome $k$ with probability $\sum_{\mu} |c_k f_{k,\mu}|^2 = |c_k|^2$, in agreement with operational quantum mechanics.

Note that this model can incorporate measurements described by positive operator-valued measures (POVMs) [44]. This follows from the fact that such measurements can be implemented by adjoining an ancilla to the system under investigation and measuring
a projector-valued measure (PVM) on the composite. By including the ancilla in our definition of the object system, the model presented above can describe these measurements. Note, however, that it is restricted to PVMs whose eigenvectors are product states with respect to the distinguished factorization.

**Further Considerations**

Despite the possibility of incorporating some POVM measurements, the model of measurement provided by Eq. (5.14) is still not the most general or realistic. Although it is true that an arbitrary state vector has many decompositions into product states with respect to the distinguished factorization, it is not necessarily the case that any of these decompositions are bi-orthogonal with respect to a coarse-graining of the distinguished factorization.

For instance, if any of the vectors in the set \(\{|\varphi_k\rangle\}_{k=1}^m\) are entangled with respect to the distinguished factor spaces of \(\mathcal{H}_S\), then theorem 2 fails to apply to \(|\psi_{\text{final}}'\rangle\). Since the problem of minimizing the IU entropy for arbitrary state vectors has not yet been solved, it is not clear what the preferred decomposition will be in this case and whether the measurement problem is resolved or not.\(^7\)

It may also occur that the evolution differs from the one assumed above in such a way that the final dynamical state vector, which we denote by \(|\psi_{\text{final}}''\rangle\), is of the same form as \(|\psi_{\text{final}}'\rangle\) except that the orthogonal set of vectors, \(\{|E_{k,\mu}\rangle\}_{\mu=1}^M\}_{k=1}^m\), is replaced by a set of vectors, \(\{|\tilde{E}_{k,\mu}\rangle\}_{\mu=1}^M\}_{k=1}^m\), that are only approximately orthogonal. Given that theorem 2 does not apply to \(|\psi_{\text{final}}''\rangle\), the question of whether or not the apparatus receives the appropriate properties in this case must also await further progress on the problem of the minimization of the IU entropy. Nonetheless, it can be shown that the minimal entropy proposal is not subject to the same objections that can be levelled against previous modal

\(^7\)It will be shown explicitly in the next section that a criterion of faithful measurement cannot be satisfied in this case, however this question is distinct from that of whether or not the measurement problem is resolved.
interpretations in this context.

For instance, consider the Vermaas-Dieks proposal. In the example described above, the reduced density operator for the apparatus is not diagonal in the basis of the $|A_{k,\mu}\rangle$, and if its eigenvalues are nearly degenerate then its eigenvectors can in fact be very different from the $|A_{k,\mu}\rangle$, as demonstrated by Bacciagaluppi, Donald and Vermaas [91]. In this case, the property assigned to the apparatus in the Vermaas-Dieks proposal can be the one associated with a projector onto a vector of the form $\sum_{k,\mu} c_{k,\mu} |A_{k,\mu}\rangle$. If the $c_{k,\mu}$ are non-zero for more than one value of $k$, then the apparatus does not receive the property associated with any projector of the form $\sum_{\mu} |A_{k,\mu}\rangle \langle A_{k,\mu}|$, and hence is not be described as indicating an outcome $k$ for any value of $k$. Given this feature, it becomes questionable whether the Vermaas-Dieks proposal solves the measurement problem.

The minimal entropy proposal is immune to this particular problem. The reason is as follows. Recall that the $|A_{k,\mu}\rangle$ were taken to be product states with respect to the distinguished factorization. Since the $|A_{k,\mu}\rangle$ for different values of $k$ correspond to macroscopically different properties, they must differ from one another in more than just one factor space. That is, a large number of the vectors in the tensor product making up $|A_{k,\mu}\rangle$ must differ from the vectors in the tensor product making up $|A_{k',\mu}\rangle$ if $k$ and $k'$ differ. As such, the vector $\sum_{k,\mu} c_{k,\mu} |A_{k,\mu}\rangle$ where the $c_{k,\mu}$ are non-zero for several values of $k$ cannot be a product state with respect to the distinguished factorization. Since the elements of the preferred decomposition are required to be product states in the minimal entropy proposal, this vector can never be an element of the preferred decomposition.

The BDD proposal is also immune to this particular problem since the vector elements of the preferred decomposition in this proposal are also product states with respect to the distinguished factorization\(^8\). However, the results of Bacciagaluppi, Donald and Vermaas [91] imply that the properties ascribed to an atomic system may depend sensitively

\(^8\)We are here assuming for simplicity that the reduced density operators of the atomic systems have no exact degeneracies.
on the exact form of the reduced density operator for that system when its eigenvalues are nearly degenerate. If such sensitive dependence existed for a large number of the atomic subsystems of the apparatus, then the macroscopic, coarse-grained properties of the apparatus, which in the BDD proposal are fixed by those of its microscopic constituents, might also have a sensitive dependence on the exact form of the state vector. As such, even if the state $|\psi'_{\text{final}}\rangle$ were associated with the apparatus indicating a definite outcome, the state $|\psi''_{\text{final}}\rangle$ might not be. The question of whether the BDD proposal has such sensitive dependence for macroscopic properties has never been examined in detail. Since the minimal entropy proposal assigns properties to atomic systems by a completely different rule, the above argument is silent about whether or not the properties of the atomic systems in the minimal entropy proposal have a sensitive dependence on the form of the state vector.

We now turn to the question of the stability over time of the set of possible macroscopic properties of the apparatus. This depends on the time dependence of the preferred decomposition, or equivalently, the nature of the preferred paths. Thus far, our model of measurement has only assumed a particular form of the dynamical state vector at a moment of time. Even if it is a good approximation to assume a model of measurement wherein at individual moments of time the dynamical state vector satisfies the conditions for the applicability of theorem 2, it is unlikely in any model that one can find a dynamical state vector that evolves unitarily and for which theorem 2 applies at every time. The reason is as follows. Bacciagaluppi, Donald and Vermaas [91] have shown that the vector elements of the bi-orthogonal decomposition may be unstable - that is, they may change significantly over a small interval of time - when the magnitude of the coefficients are nearly degenerate. Given that most of the states in a Hilbert space are entangled states, if these vector elements are product states at one time it is highly unlikely that they will be product states at a later time. Thus, even if theorem 2 applies at one time, it is highly unlikely that it will apply at a later time. In the absence of the applicability of theorem
2, we cannot at present make any statements about the nature of the minimal entropy product decomposition. As such, we see that the question of the stability of the set of possible macroscopic properties of the apparatus must also remain open for the moment.

Finally, we note that the assumption that the apparatus and environment are initially unentangled is also an unrealistic feature of the standard model of measurement. For that matter, the assumption that the composite of system, apparatus and environment is unentangled with the rest of the universe may not be realistic either. However, this difficulty is not unique to the minimal entropy proposal. Every realist no-collapse interpretation must contend with the fact that the dynamical state vector for the universe is in general not factorizable with respect to subsystems that have interacted in the past, even if this interaction is quite weak. Further work is required to determine whether the predictions of the minimal entropy proposal remain satisfactory when these assumptions are relaxed.

5.4.2 Sequences of measurements

We now demonstrate the extent to which the minimal entropy proposal is in agreement with operational quantum mechanics for sequences of measurements. Consider in particular a sequence of two measurements. Suppose that the first measurement is of a variable $V$ with eigenstates \{\ket{\varphi_k}\}_{k=1}^m$, and that the second measurement is of a variable $V'$ with eigenstates \{\ket{\varphi'_k}\}_{k=1}^m$. Suppose moreover that upon obtaining outcome $k$ for the first measurement, the state $|\tilde{\varphi}_k\rangle$ is prepared, where the set \{\ket{\tilde{\varphi}_k}\}_{k=1}^m although normalized, may be non-orthogonal. If $|\tilde{\varphi}_k\rangle \neq |\varphi_k\rangle$ for one or more values of $k$, the first measurement is said to be disturbing.

In the last subsection we considered two distinct models of measurement which differed in the extent to which the apparatus and the environment became entangled due to their interaction. In this subsection, we consider only the simpler of the two models. The reader can verify that the more realistic model leads to the same conclusions.
There are now two apparatuses, and an environment for each. We denote their Hilbert spaces by $\mathcal{H}^{A_1}, \mathcal{H}^{A_2}, \mathcal{H}^{E_1},$ and $\mathcal{H}^{E_2}$ respectively, and we distinguish state vectors for the two apparatuses (environments) by a superscript. It is again assumed that the object system, the two apparatuses and the two environments are all initially uncorrelated. The distinguished factorization $F$ is assumed to have $\{\mathcal{H}^S, \mathcal{H}^{A_1}, \mathcal{H}^{A_2}, \mathcal{H}^{E_1}, \mathcal{H}^{E_2}\}$ as a coarse-graining.

We assume that the first measurement is well described by Eq. (5.12) with the exception of a change of notation: $|A_0\rangle, |E_0\rangle, |A_k\rangle$ and $|E_k\rangle$ become $|A_0^1\rangle, |E_0^1\rangle, |A_k^1\rangle$ and $|E_k^1\rangle$ in order to specify that the object system interacts with the first rather than the second apparatus. We assume that the second apparatus and its environment remain uncorrelated with the rest of the system and each other during this first measurement. It follows that the dynamical state vector for the total system after the first measurement is

$$
|\psi_{\text{final 1}}\rangle = \left( \sum_{k=1}^{m} c_k |\tilde{\phi}_k\rangle \otimes |A_k^1\rangle \otimes |E_k^1\rangle \right) \otimes |A_0^2\rangle \otimes |E_0^2\rangle . \tag{5.15}
$$

Supposing that $\{|\tilde{\phi}_k\rangle\}_{k=1}^{m}$, $\{|A_k^1\rangle\}_{k=1}^{m}$, $\{|E_k^1\rangle\}_{k=1}^{m}$, $|A_0^2\rangle$ and $|E_0^2\rangle$ are product states with respect to $F$, if we use the bi-partite factorization $\{\mathcal{H}^S \otimes \mathcal{H}^{A_1} \otimes \mathcal{H}^{A_2}, \mathcal{H}^{E_1} \otimes \mathcal{H}^{E_2}\}$ in place of the bi-partite factorization $\{\mathcal{H}^S \otimes \mathcal{H}^A, \mathcal{H}^E\}$ in the arguments found in the previous subsection, then it is straightforward to show that the preferred decomposition of $|\psi_{\text{final 1}}\rangle$ is

$$
D_{\text{final 1}} = \left\{ (c_k, |\tilde{\phi}_k\rangle \otimes |A_k^1\rangle \otimes |E_k^1\rangle \otimes |A_0^2\rangle \otimes |E_0^2\rangle) \right\}_{k=1}^{m} . \tag{5.16}
$$

We conclude that with probability $|c_k|^2$, the first apparatus indicates outcome $k$, while the second apparatus remains ready to measure.

Now assume that the second measurement is also well described by Eq. (5.12) with the notational change that $|A_0\rangle, |E_0\rangle, |A_k\rangle$ and $|E_k\rangle$ become $|A_0^2\rangle, |E_0^2\rangle, |A_k^2\rangle$ and $|E_k^2\rangle$ since the object system is now interacting with the second apparatus, and where the vectors for the object system acquire a prime since the second measurement is of $V'$
rather than $V$. For simplicity, we take this second measurement to be non-disturbing, so that $|\varphi'_k\rangle = |\varphi'_k\rangle$. Assume also that the first apparatus and its environment have no interactions during this measurement. It then follows that the dynamical state vector after the second measurement is

$$
|\psi_{\text{final} 2}\rangle = \sum_{k=1}^{m} \sum_{j=1}^{m} c_k d_j^k |\varphi'_j\rangle \otimes |A_k^1\rangle \otimes |E_k^1\rangle \otimes |A_j^2\rangle \otimes |E_j^2\rangle , \tag{5.17}
$$

where the coefficients $\{d_j^k\}_{j=1}^{m}$ are defined by $|\tilde{\varphi}_k\rangle = \sum_{j=1}^{m} d_j^k |\varphi'_j\rangle$. Again, if we suppose that $\{|\varphi'_j\rangle\}_{j=1}^{m}, \{|A_j^2\rangle\}_{j=1}^{m}$ and $\{|E_j^2\rangle\}_{j=1}^{m}$ are product states with respect to $F$ and if we use the bi-partite factorization $\mathcal{H}^S \otimes \mathcal{H}^{A1} \otimes \mathcal{H}^{A2}, \mathcal{H}^{E1} \otimes \mathcal{H}^{E2}$ in place of the bi-partite factorization $\mathcal{H}^S \otimes \mathcal{H}^{A}, \mathcal{H}^{E}$ in all the arguments found in the previous subsection, the preferred decomposition of $|\psi_{\text{final} 2}\rangle$ is found to be

$$
D_{\text{final} 2} = \left\{ \left( c_k d_j^k, |\varphi'_j\rangle \otimes |A_k^1\rangle \otimes |E_k^1\rangle \otimes |A_j^2\rangle \otimes |E_j^2\rangle \right) \right\}_{k=1}^{m} . \tag{5.18}
$$

We can therefore conclude that there is a probability $|c_k d_j^k|^2$ that the first apparatus indicates outcome $k$ and the second apparatus indicates outcome $j$ after the second measurement. It follows that the probability of the second apparatus indicating outcome $j$ given that the first apparatus indicates outcome $k$ after the second measurement is $|d_j^k|^2 = |\langle \varphi'_j|\tilde{\varphi}_k\rangle|^2$.

However, we have still not determined the probability for the second apparatus to indicate outcome $j$ after the second measurement, given that the first apparatus indicates outcome $k$ after the first measurement; this is the quantity specified by operational quantum mechanics. The problem is that it has not been shown that the outcome indicated by the first apparatus is stable over time. Whether it is or not depends on the dynamics of the property state vector, which is determined by Eqs. (5.10) and (5.11). As pointed in the previous subsection, for any sensible model of measurement we cannot at present determine the time-sequence of preferred decompositions nor the preferred paths...
through Hilbert space defined by this sequence. Since Eqs. (5.10) and (5.11) depend on the identity of these preferred paths, we cannot at present determine the dynamics of the property state vector.

Thus, it remains to be shown that within the minimal entropy proposal the apparatus is never described as 'jumping' between macroscopically different readings, that is, that the actual macroscopic properties of the apparatus are stable over time. However, given such stability, the minimal entropy proposal reproduces the predictions of operational quantum mechanics within the model of measurement we are considering. For the arguments in the rest of the chapter, we must assume that such stability holds.

5.5 The Faithfulness criterion

In the preceding section, we focused upon the properties of the measurement apparatus. Presently, we wish to consider the properties assigned to the microscopic system under investigation. If the properties of such microscopic systems are to play any explanatory role in the theory, then one would expect their role to be in determining the outcomes of measurements upon them. In particular, one might expect that at the least, measurements that are perfectly predictable reveal pre-existing properties. Specifically, one might expect the following condition to hold:

**Faithfulness Criterion** If it can be predicted with probability 1, using operational quantum mechanics, that a measurement associated with the variable $V$ will yield the result $v$, then immediately prior to the measurement the variable $V$ is determinate with value $v$.

A more detailed motivation for this criterion is provided in SS. Modal interpretations that make use of the bi-orthogonal rule typically satisfy this criterion for ideal (von Neumann) measurements. Nonetheless, both the Kochen-Dieks and the atomic modal interpretation fail to do so for certain non-ideal measurements, as we now demonstrate.
Consider an experiment involving a sequence of two measurements, such as the one discussed in the previous section. Suppose that the first measurement is disturbing and corresponds to a preparation associated with the vector $|\tilde{\varphi}_k\rangle$ when the outcome $k$ is obtained, and that the set of states $\{|\tilde{\varphi}_k\rangle\}_{k=1}^m$ are non-orthogonal. Suppose moreover that the second measurement is of the projector onto one of these states, say $P_{\tilde{\varphi}_k^*} \equiv |\tilde{\varphi}_{k^*}\rangle \langle \tilde{\varphi}_{k^*}|$. In this case, upon obtaining the outcome $k^*$ for the first measurement, it can be predicted with probability 1 that the outcome of the measurement of $P_{\tilde{\varphi}_{k^*}}$ will be 1. It follows from the faithfulness criterion that $P_{\tilde{\varphi}_{k^*}}$ must be determinate and receive the value 1 immediately prior to the second measurement.

We shall again consider only the simpler of the two theoretical models of the measurement interaction presented in section 5.4; it is straightforward but tedious to show that the following results also apply for the more sophisticated model. The dynamical state vector immediately prior to the second measurement has the form of $|\psi_{\text{final}}\rangle$, defined in Eq. (5.15). In the VD proposal, the variables that are determinate for a system are those which have as eigenstates all the elements in the spectral resolution of the reduced density operator for the system. Given that the spectral resolution is necessarily orthogonal, and given that the set of states $\{|\tilde{\varphi}_k\rangle\}_{k=1}^m$ are non-orthogonal, not all of these states can appear in the spectral resolution of the density operator for the system under investigation. In particular, the vector $|\tilde{\varphi}_{k^*}\rangle$ need not appear, in which case the projector $P_{\tilde{\varphi}_{k^*}}$ need not be determinate. Consequently, the VD proposal fails to satisfy the faithfulness criterion in this example. This conclusion can be also be seen to follow from an argument made by Bacciagaluppi and Hemmo [85]. The BDD proposal exhibits a similar failure if the Hilbert space of the system under investigation, $\mathcal{H}^S$, is an element of the distinguished factorization.

In contrast, the minimal entropy proposal does satisfy the faithfulness criterion for this example. As was shown in the previous section, the preferred decomposition of $|\psi_{\text{final}}\rangle$, denoted $D_{\text{final}}$, is given by Eq. (5.16). If the first apparatus indicates the
outcome $k^*$ at time $t$, the property state vector must be the $k^*$th element of $D_{\text{final}}$, that is, $|\Phi_{\text{final}}\rangle = |\tilde{\varphi}_k\rangle \otimes |A_{k^*}^1\rangle \otimes |E_{k^*}^1\rangle \otimes |A_0^2\rangle \otimes |E_0^2\rangle$, in which case the projector $P_{\tilde{\varphi}_k^*}$ is determinate and receives the value 1.

It should be noted that the ability of the minimal entropy proposal to satisfy the faithfulness criterion in this example is a result not only of the choice of preferred decomposition, but also the fact that this choice was incorporated into the framework for modal interpretations that was developed in SS. The same choice of preferred decomposition within the Bub-Clifton framework would not exhibit faithfulness. The reason is as follows. Although Bub-Clifton also adopt the reductionist rule, they do not assume that the variables that are determinate for the universe are those that have the property state vector (defined in section 5.3) as an eigenstate. Rather, in the Bub-Clifton framework, the variables that are determinate are those that have all of the elements of the preferred decomposition as eigenstates. In the example we are considering, it follows from the reductionist rule that only variables that have all of the states $\{|\tilde{\varphi}_k\rangle\}_{k=1}^n$ as eigenstates are determinate for the system. But given that these states can be non-orthogonal, they need not all be eigenstates of $P_{\tilde{\varphi}_k^*}$, and thus $P_{\tilde{\varphi}_k^*}$ need not be determinate.

We end this section by considering a measurement of a variable whose eigenstates are not all product states with respect to the distinguished factorization $F$. For such measurements, the faithfulness criterion cannot be satisfied within the minimal entropy proposal. The reason is as follows. Suppose $|\varphi\rangle$ is an eigenstate of the measured variable that is entangled with respect to $F$. If a preparation of $|\varphi\rangle$ is followed by a measurement of the projector $P_\varphi \equiv |\varphi\rangle \langle \varphi|$, then the outcome is perfectly predictable, and the faithfulness criterion requires that the projector $P_\varphi$ be determinate with value 1 immediately prior to the measurement. However, for this to occur the property state vector must be an eigenstate of $P_\varphi$, and hence must be entangled with respect to $F$. But the property state vector is always a product state with respect to $F$ in the minimal entropy proposal. The failure of the faithfulness criterion for such measurements is a consequence of the fact...
that the preferred decomposition is a product decomposition. As such, it also occurs for the BDD proposal, as discussed by Dieks [39] and also by Vermaas [87].

5.6 Conclusions

We have presented a novel proposal for the preferred decomposition. It is assumed that there is a distinguished set of subsystems of the universe, that is, a distinguished factorization of the total Hilbert space into a tensor product of Hilbert spaces, and that the preferred decomposition is a product decomposition with respect to this factorization. In the case of a distinguished factorization that is bi-partite, there is a product decomposition that stands out from among the rest: the bi-orthogonal decomposition. However, the obvious generalization of the bi-orthogonal decomposition to an n-partite distinguished factorization, namely the n-orthogonal decomposition, does not exist for all state vectors, as shown by Peres [90]. The decomposition we suggest is equal to the n-orthogonal decomposition when the latter exists, but continues to exist when the latter does not. As such, it can be thought of as a natural generalization of the bi-orthogonal decomposition to n-partite systems. Specifically, we have proposed that the preferred decomposition be the one that minimizes the IU entropy from among all product decompositions with respect to the distinguished factorization.

By construction, the minimal entropy proposal does not suffer from perspectivalism. Moreover, we have shown that it has some success in dealing with the quantum measurement problem and in satisfying the faithfulness criterion. The measurement problem is resolved for measurements of variables with eigenstates that are product states with respect to the distinguished factorization, assuming particular microscopic models of the apparatus and environment. Within the same microscopic models, the faithfulness criterion is satisfied for sequences of measurements, the first of which may be disturbing and the second of which measures a variable with eigenstates that are product states with
There remain many unanswered questions in the minimal entropy proposal, the foremost being the question of what decomposition minimizes the IU entropy when theorem 2 does not apply. The answer to this question will determine whether one can solve the quantum measurement problem for more general types of measurements than the ones considered here, for example, measurements of variables with eigenstates that are entangled with respect to the distinguished factorization. In addition, such progress is required to determine what the proposal has to say about more realistic models of measurements, such as models wherein the states of the environment that are relative to different pointer states of the apparatus are only approximately orthogonal, and models that take into account the pre-existing entanglement between the systems of interest and the rest of the universe.

The general solution of the entropy minimization problem will also tell us whether a set of continuous preferred paths can be defined from the time sequence of preferred decompositions, whether an extended non-uniqueness is forbidden for a system undergoing Hamiltonian evolution, and whether the set of states for which the preferred decomposition is non-unique is a set of measure zero in the set of all states in the Hilbert space. If the answers to all these questions are affirmative, then the only non-uniqueness in the preferred decomposition occurs at isolated moments in time, and the properties at these moments can be defined by appealing to the limit of the preferred paths at these moments.

Finally, progress on the minimization problem will answer two questions that concern, respectively, the dynamics of the preferred decomposition and the dynamics of the property state vector. The first question is whether the preferred paths yield sensible properties for the apparatus at all times for realistic models of measurement. Previous modal interpretations have faced serious difficulties on this front. In both the VD and BDD proposals there is a sensitive dependence of properties on the form of the dynam-
ical state vector. This feature can threaten the solution of the measurement problem if macroscopic properties vary widely under small variations in the model of measurement or small variations in time. We have shown that the arguments establishing the existence of such sensitive dependence for the VD and BDD proposals do not apply to the minimal entropy proposal. Although this result is promising, it remains to be shown that such sensitive dependence is in fact absent from the minimal entropy proposal, or at least that it is absent for macroscopic properties. The second question is whether the generalized Schrödinger dynamics, or indeed, any choice of dynamics for the property state vector, predicts that the actually possessed properties of an apparatus are stable over time.

One of the goals of our interpretational endeavour was to obtain faithfulness for certain kinds of measurements, in particular, sequences of measurements the first of which is disturbing. As was shown in the previous section, the minimal entropy proposal achieves this goal if the second measurement is of a variable whose eigenstates are product states with respect to the distinguished factorization. However, the faithfulness criterion explicitly fails to be satisfied in any measurement of a variable whose eigenstates are entangled with respect to the distinguished factorization.

This result is perhaps not surprising, since it is the assumption that the preferred decomposition be a product decomposition with respect to the distinguished factorization which is the source of the problem, and this assumption seems critical to solving the measurement problem. Indeed, it may be that the requirement of empirical adequacy rules out the possibility of satisfying the faithfulness criterion for any interpretation that fits within the generalized framework presented in SS and used here. Specifically, one could argue as follows. There is nothing within operational quantum mechanics which prohibits a measurement upon a composite of system, apparatus and environment that verifies that the state vector is of the form of Eq. (5.13). If the initial preparation were associated with this state vector, then the outcome of the measurement would be perfectly predictable, and thus the faithfulness criterion would imply that the composite
must have the property associated with the projector onto this state. However, in this case the property corresponding to the apparatus indicating a particular outcome would not be possessed, in contradiction with the predictions of operational quantum mechanics.

One could argue that such measurements may, in fact, be impossible to implement, so that the faithfulness criterion might remain consistent with solving the measurement problem. For instance, Omnès has argued that the type of measurement we are imagining could not be done, since the measurement apparatus would have to contain more matter than is contained in the known universe [94]. Such arguments leave open the possibility that the minimal entropy proposal still satisfies the faithfulness criterion for all measurements that can be physically implemented. Specifically, it may be that there exists a distinguished factorization such that measurements of observables that were entangled with respect to this factorization were simply not possible given the specific features of the universe in which we live. Despite the logical possibility of such a resolution, none suggests itself at this time.

Perhaps a more reasonable response to this apparent conflict between faithfulness and empirical adequacy in the generalized framework for modal interpretations is to conclude that faithfulness cannot be a feature of all measurements. The fact that the outcomes of some perfectly predictable measurements cannot be explained in terms of pre-existing properties makes one wonder whether any perfectly predictable measurements should be explained in this way. We feel that an interpretation that satisfies faithfulness to as great an extent as possible has some appeal, since if nothing else, it accords in as many cases as possible with the description of microscopic systems that is provided by a ‘standard’ view wherein the state vector undergoes a collapse after a measurement upon the system.

As mentioned in the Introduction, the use of a preferred decomposition, sometimes called an ‘interpretation basis’, has been viewed by some as necessary within interpretive strategies distinct from modal interpretations, such as many-worlds, consistent histories, and collapse theories. Thus, the preferred decomposition of the minimal entropy pro-
positional may well be of relevance to such interpretive strategies as well. In any event, a mathematically precise proposal, even though not without problems, can be useful in stimulating progress on interpretive issues, as is evidenced by the recent profusion of work on modal interpretations. We hope that the minimal entropy proposal will not be an exception in this respect.
Chapter 6

Conclusions and future directions

In this thesis, we have presented theoretical studies of selected topics in quantum cryptography, Bose-Einstein condensation and the interpretation of quantum mechanics, each of which has constituted an investigation into the consequences of non-factorizable quantum states. We presently review our most significant results, discuss the future research which they suggest, and draw some connections between these seemingly disparate "aspects of entanglement."

No bit commitment protocol can be both arbitrarily concealing and arbitrarily binding. This is the Mayers-Lo-Chau theorem. It is a consequence of non-factorizable quantum states with profound implications for quantum cryptography. Many cryptographic tasks, once thought to be possible due to a mistaken belief in the possibility of arbitrarily secure BC, are now being re-examined to determine how much security can really be achieved. It is clear that knowing the maximum degree of security that can be achieved in BC will be important in this endeavour. In chapters 2 and 3 of this thesis we have investigated this problem in detail. Our most significant result is that a linear trade-off between concealment and bindingness is the optimal trade-off for the class of Alice-supplied BC protocols, and that a family of purification BC protocols achieves this trade-off.

There remain several important open questions. For one, we have not yet determined
whether there are any other protocols, besides the purification BC protocols, which can achieve the optimal trade-off among Alice-supplied BC protocols, in particular, whether this can be accomplished with generalized BB84 BC protocols. This is an important question because in practice it is much easier to implement a protocol for which the honest strategies do not require the ability to generate entangled states. The second and more important question is whether the linear trade-off is optimal overall.

In addition to optimizing over protocols, we have considered the optimization of coherent attacks in specific classes of protocols. This topic holds interest beyond its relevance for the security of bit commitment, since coherent attacks are an example of a more general task, namely, the preparation of quantum states at a remote location. The results of chapters 2 and 3 therefore find their broader significance in elucidating how entanglement can be used as a resource for this task.

One can define many variants on the task of remote state preparation, depending on what the 'preparer' knows about the state to be prepared, whether the parties involved in its implementation are cooperative or adversarial, and how much resource material is available, such as the number of classical or quantum bits that can be exchanged, and the amount of prior entanglement the parties share. Bennett et al. [95] have recently considered remote state preparation in the case of cooperative parties who share prior entanglement and a classical channel when the preparer has full classical information about the state to be prepared. In the type of remote state preparation we have considered here, the parties are adversarial rather than cooperative. In generalized BB84 BC protocols, Alice must remotely prepare a pure state drawn from one of two sets. In purification BC protocols, Alice's task can be described as remotely preparing one of two mixed states; although Bob cannot verify that Alice submitted a particular mixed state by performing measurements upon his system alone, he can do so by demanding that Alice provide him with a purification of this mixed state, and then measuring for this purification. In both cases, Alice can choose to prepare any entangled state she wishes,
but she must make this choice at a time prior to knowing which state she would like to prepare.

It seems to us that the primitive of remote state preparation, construed in its most general sense, may be as fundamental as the primitive of state estimation and just as significant for the purposes of determining what sorts of information processing tasks can be successfully implemented using quantum systems. The mapping, presented in chapter 2, between a particular kind of state estimation and part of the remote state preparation task that is relevant for coherent attacks, suggests that there may be other connections between these two problems. A promising avenue of future research is to explore this analogy in more detail.

In chapter 4, we demonstrated an effect that can be used to prepare states of varying degrees of entanglement between spatially separated modes of a Bose-Einstein condensate. In particular, we showed that for a condensate of atoms with weak repulsive inter-particle interactions trapped in a double-well potential, the variance in the relative number between the two wells could be squeezed to various degrees by varying the height of the central barrier and allowing the atoms to relax to their ground state. In 1998 we discussed these results with Prof. M. Kasevich whose group performs experiments on condensates trapped in a one-dimensional optical lattice. Such traps provide a chain of potential wells, the depths of which can be experimentally controlled by varying the intensity of the trapping laser. Although the atoms are spread over approximately 12 lattice sites in their experiment, so that one has a multiple well rather than simply a double well, the physics in the two cases is essentially the same, and in the March 2001 issue of Science, Kasevich's group reported having observed the effect we describe [97].

Given our emphasis upon the significance of entanglement as a resource for physical tasks, an obvious question to ask about the entangled states discussed in chapter 4 is whether these are useful for anything besides the high-precision interferometry mentioned in the introduction. In particular, the reader may be wondering whether such states can
be used to implement the purification BC protocol discussed in chapter 3.

We do not have an answer to this question at present. Note however that the task of implementing Bob's honest strategy in a purification BC protocol requires the ability to verify that a pair of systems is in a particular entangled state, and we do not know at present of any way to perform such a measurement for the states studied in chapter 4. There is also reason to be sceptical that such states will be useful for other tasks that are implemented between spatially separated parties. We do not need to go into the details of any of these tasks to exhibit the problem; it suffices to note that many of these require the parties to be able to perform measurements and unitary transformations that are referenced to the same basis in Hilbert space. This means sharing a common reference frame for the degree of freedom being manipulated. For instance, if the parties are using spins they will have to agree on a direction in space, perhaps by referencing their measurement to a distant star. If they are working with non-degenerate energy eigenstates, they will require synchronized clocks [96]. The degree of freedom that must be manipulated by parties using the entangled states of chapter 4 is the occupation number of an atomic mode. Since different occupation numbers have energies which differ by the rest mass of the atom, these parties will require clocks synchronized at frequencies corresponding to this energy scale. However, it is unclear whether it is possible at present to even establish clock synchronization at optical frequencies, let alone frequencies associated with the rest mass of an atom.

These considerations suggest an interesting direction of future research, namely, to explore the differences between entanglement in Fock space and entanglement in configuration space. This issue appears to be related to the role of time as an observable in quantum mechanics, which, like entanglement, remains poorly understood.

In chapter 5, we proposed a modal interpretation of quantum mechanics based on a novel choice of preferred decomposition of the state vector: from among all decompositions containing only product states with respect to a distinguished factorization of the
total Hilbert space, we choose the one for which the coefficients squared have the smallest Shannon entropy. This proposal was shown to compare favorably with its predecessors, specifically, in the extent to which it provides a solution to the quantum measurement problem.

There remains much research to be done in order to properly assess this proposal. The most significant outstanding problem is the identification of the product decomposition that minimizes the IU entropy for arbitrary state vectors. Only once this variational problem is addressed will it be possible to determine whether this interpretation solves the measurement problem in general. This problem may well prove to be mathematically very challenging. However, much progress is currently being made on the quantification of entanglement [9], and it is likely that the mathematical tools that will be found to be useful in this context will be useful for our problem as well. Another way in which these results make a connection with quantum information theory is that the minimal IU entropy may itself constitute a measure of multi-partite entanglement. Moreover, the 'canonical decomposition' which we have proposed may be useful for quantum information theorists in the same way that the bi-orthogonal decomposition has proved to be useful. A comparison of our proposal with other multi-partite generalizations of the bi-orthogonal decomposition has been made by Carteret et al. [98], however not much can be concluded about the relative merits of these decompositions at present.

We have studied entanglement in the context of both practical applications and foundational issues. We end with some thoughts on the interplay between these two approaches.

It is a fair assessment, in our opinion, that the rapidly growing field of quantum information theory finds its origins partly in investigations into the foundations of quantum mechanics. In particular, John Bell's work on local hidden variable theories [3] provided one of the first hints that quantum mechanics permits the implementation of information-theoretic tasks that are impossible classically.
It may be, however, that the flow of ideas in the near future will be primarily in
the other direction, that is, that progress in the field of quantum information theory
will stimulate progress in the field of foundations. For instance, Chris Fuchs and Gilles
Brassard have conjectured [99] that the postulates of quantum mechanics might be de-
rived from two information-theoretic assumptions: (1) that key distribution is possible
and (2) that bit commitment which is arbitrarily concealing and binding is impossible.
Although this particular conjecture may well be incorrect, the general idea is appeal-
ing: rather than assuming that the universe is governed by quantum mechanics and
asking which information-theoretic tasks are possible, assume that the universe is a place
wherein certain information-theoretic tasks are possible and ask what sort of physical
theory would have to govern such a universe. If one identified a few simple information-
theoretic principles from which the entire structure of quantum mechanics followed, then
this would constitute an accomplishment similar to Einstein's derivation of the Lorentz
transformations from a pair of physical principles [100].

Even if one cannot identify principles which imply all of the structure of quantum
mechanics, one might still be able to do so for some of the theory's features. For instance,
it may be that the necessity of entanglement, or equivalently, of a tensor product structure
on the space of states, follows from simple assumptions about the possibility of certain
information-theoretic tasks.

In brief, progress in quantum information theory may help secure a deeper under-
standing of the structure of quantum mechanics, and a deeper understanding of the
structure of quantum mechanics may yet lead to a consensus on its interpretation.
Appendix A

Proof of results of section 2.6.3

We here provide the proof of optimality of the convex decomposition specified by Eq. (2.9). First, we establish the applicability of Jaynes' rule, defined in Eq. (2.2), to the probabilities in the optimal convex decomposition. This requires showing that the optimal decomposition is an extremal decomposition with the number of positively-weighted elements equal to the rank of $\rho$.

This is trivial to see for a pure $\rho$. We now demonstrate it for an impure $\rho$. Because we have assumed that the $\{\psi_k\}_{k=1}^n$ are linearly independent, they span the whole 2D Hilbert space, and because $\rho$ has rank 2, its support is the 2D Hilbert space. Thus, the $\{\psi_k\}_{k=1}^n$ are linearly independent and have a span that is equal to the support of $\rho$, which, as shown in section 2.5.1 by the mapping to the state estimation problem, is sufficient to establish that the optimal convex decomposition is an extremal decomposition. It was shown in section 2.4 that the number of positively-weighted elements in the optimal convex decomposition is less than or equal to $n$. In the present case, $n = 2$, so this number must be less than or equal to 2. However, since $\rho$ is impure, every convex decompositions of $\rho$ has at least 2 elements receiving non-zero probability. Thus, the number must be precisely 2, which is the rank of $\rho$.

Jaynes’ rule provides a formula for the probabilities in a convex decomposition of $\rho$
in terms of \( \rho \) and the elements in the decomposition. In terms of Bloch vectors, it has the form

\[
q_k = \frac{1}{2} \left( 1 - \frac{|\vec{r}|^2}{1 - \vec{r} \cdot \hat{s}_k} \right),
\]

where we have written \( \hat{s}_k \) rather than \( \tilde{s}_k \) since the elements of the optimal decomposition, being pure, can be represented by unit Bloch vectors. Substituting this expression, together with the constraint that \( \vec{r} = q_1 \hat{s}_1 + q_2 \hat{s}_2 \) into Eq. (2.8), we can write \( P_{Ub} \) entirely in terms of \( \hat{s}_1 \),

\[
P_{Ub} = \frac{1}{2} \left( 1 + \frac{q_1 (\hat{a}_1 \cdot \hat{s}_1) + (\hat{a}_2 \cdot \vec{r}) - q_1 (\hat{a}_2 \cdot \hat{s}_1)}{1 - |\vec{r}|^2} \right).
\]

Rather than varying this quantity with respect to \( \hat{s}_1 \), we vary with respect to an un-normalized vector \( \bar{s}_1 \), taking \( \hat{s}_1 = \bar{s}_1 / |\bar{s}_1| \), where \( |\bar{s}_1| = \sqrt{\vec{s}_1 \cdot \vec{s}_1} \). Setting \( \delta P_{E}(\hat{s}_1) = 0 \) and making use of the fact that \( \delta |\bar{s}_1| = \delta \sqrt{\vec{s}_1 \cdot \vec{s}_1} = \delta \vec{s}_1 \cdot \vec{s}_1 \), we find that the optimal \( \hat{s}_1 \) satisfies

\[
(1 - \hat{s}_1 \cdot \vec{r}) (\hat{a}_1 - \hat{a}_2) + (\hat{s}_1 \cdot (\hat{a}_1 - \hat{a}_2)) (\vec{r} - \hat{s}_1) = 0.
\]

By assumption, \( |\vec{r}| \neq 1 \) (since \( \rho \) is impure). It follows that \( (1 - \hat{s}_1 \cdot \vec{r}) \neq 0 \), and \( (\vec{r} - \hat{s}_1) \neq \vec{0} \). Since it is also the case that \( (\hat{a}_1 - \hat{a}_2) \neq \vec{0} \), we infer that \( \hat{s}_1 \cdot (\hat{a}_1 - \hat{a}_2) \neq 0 \). Taking the dot product of this equation with \( \hat{a}_1 + \hat{a}_2 \), we find

\[
(\vec{r} - \hat{s}_1) \cdot (\hat{a}_1 + \hat{a}_2) = 0.
\]

Consequently, the solutions that extremize \( P_{Ub} \) are of the form

\[
\hat{s}_{1 \pm}^{ext} = \vec{r} + L_{\pm} (\vec{r}) \hat{d},
\]

where \( \hat{d} \) is given in Eq. (2.3). The constraint \( |\hat{s}_{1 \pm}^{ext}| = 1 \) implies that \( L_{\pm} (\vec{r}) \) have the form
specified in Eq. (2.11). Plugging $\hat{s}^{\text{ext}}_{1\pm}$ into the expression for $P_{Ub}$, we find

$$P_{Ub} = \frac{1}{2} \left( 1 + \hat{a}_1 \cdot \hat{r} + L_{\pm}(\hat{r}) \left( \hat{a}_1 \cdot \hat{d} \right) \right).$$

Since the coefficient of $L_{\pm}(\hat{r})$ is positive, and $L_{+}(\hat{r}) \geq L_{-}(\hat{r})$, the maximum $P_{Ub}$ occurs for $\hat{s}^{\text{ext}}_{1+}$, while the minimum occurs for $\hat{s}^{\text{ext}}_{1-}$. Thus, the optimal $\hat{s}_1$ given $\hat{r}$ is

$$\hat{s}^{\text{opt}}_1 = \hat{r} + L_{+}(\hat{r}) \hat{d}.\$$

The constraint $\hat{r} = \sum_k q_k \tilde{s}_k$ then implies that

$$\hat{s}^{\text{opt}}_2 = \hat{r} + L_{-}(\hat{r}) \hat{d}.$$

This establishes what we set out to prove.
Appendix B

Proof of results of section 2.6.4

We here provide the proofs of all the results presented in section 2.6.4.

Proof for case 1. The parallel condition is equivalent to \( \dot{d}_0 = \dot{d}_1 \) which implies that \( L_{0+} = L_{1+} \), so that Eq. (2.13) becomes

\[
P_U = \frac{1}{2} + \frac{1}{4} \left( \vec{r} + L_{0+} (\vec{r}) \dot{d}_0 \right) \cdot (\dot{a}_1^0 + \dot{a}_1^1).
\]

This is maximized for \( \vec{r} + L_{0+} (\vec{r}) \dot{d}_0 = \frac{\dot{a}_1^0 + \dot{a}_1^1}{|\dot{a}_1^0 + \dot{a}_1^1|} \), which implies that \( \vec{r}^{\text{opt}} \) can be any vector of the form specified in Eq. (2.14). \( \Box \)

Proof for case 2. Starting from Eq. (2.13), we extremize \( P_U \) with respect to variations in \( \vec{r} \) by setting \( \delta P_U(\vec{r}) = 0 \). Using the fact that \( \delta \vec{r} = \delta \sqrt{\vec{r} \cdot \vec{r}} = \delta \vec{r} / r \), and

\[
\delta L_{b+} (\vec{r}) = - \left( \frac{\vec{r} + L_{b+} (\vec{r}) \dot{d}_b}{\vec{r} \cdot \dot{d}_b + L_{b+} (\vec{r})} \right) \cdot \delta \vec{r},
\]

we find that the extremal \( \vec{r} \) satisfy

\[
\sum_{b=0}^{1} \left( \dot{a}_1^b - (\dot{d}_b \cdot \dot{a}_1^b) \left( \frac{\vec{r} + L_{b+} (\vec{r}) \dot{d}_b}{\vec{r} \cdot \dot{d}_b + L_{b+} (\vec{r})} \right) \right) = 0. \tag{B.1}
\]
We now introduce the notation

\begin{align*}
x_0 &= \vec{r} \cdot \hat{d}_1^+ \\
x_1 &= \vec{r} \cdot \hat{d}_0^+ \\
x_2 &= \vec{r} \cdot \hat{n},
\end{align*}

where \( \hat{d}_1^+ \), \( \hat{d}_0^+ \) and \( \hat{n} \) are defined in Eq. (2.18). Making use of the fact that \( \vec{r} = (\vec{r} \cdot \hat{d}_0) \hat{d}_0 + (\vec{r} \cdot \hat{d}_0^+) \hat{d}_0^+ + (\vec{r} \cdot \hat{n}) \hat{n} \), we have \( \left( \frac{\vec{r} + L_{0+}(\vec{r}) \hat{d}_0}{\vec{r} \cdot \hat{d}_0 + L_{0+}(\vec{r})} \right) = \hat{d}_0 + \frac{x_1 \hat{d}_1^+ + x_2 \hat{n}}{\sqrt{1 - x_1^2 - x_2^2}} \) which together with \( \hat{a}_1^0 = (\hat{a}_1^0 \cdot \hat{d}_0) \hat{d}_0 + (\hat{a}_0^0 \cdot \hat{d}_0^+) \hat{d}_0^+ + (\hat{a}_0^0 \cdot \hat{n}) \hat{n} \) yields

\[
\hat{a}_1^0 - (\hat{d}_0 \cdot \hat{a}_1^0) \left( \frac{\vec{r} + L_{0+}(\vec{r}) \hat{d}_0}{\vec{r} \cdot \hat{d}_0 + L_{0+}(\vec{r})} \right) = \\
(\hat{a}_1^0 \cdot \hat{d}_0^+) \hat{d}_0^+ + (\hat{a}_0^0 \cdot \hat{n}) \hat{n} - \frac{(\hat{d}_0 \cdot \hat{a}_1^0)}{\sqrt{1 - x_1^2 - x_2^2}} (x_1 \hat{d}_1^+ + x_2 \hat{n}).
\]

An analogous result holds for \( b = 1 \). Plugging these expressions into Eq. (B.1) and taking the dot product with each of \( \hat{d}_0, \hat{d}_1 \) and \( \hat{n} \), we obtain the set of equations

\[
\begin{align*}
0 &= (\hat{a}_1^0 \cdot \hat{d}_1^+) \sqrt{1 - x_0^2 - x_2^2} - (\hat{a}_1^1 \cdot \hat{d}_1) x_0, \\
0 &= (\hat{a}_0^0 \cdot \hat{d}_0^+) \sqrt{1 - x_1^2 - x_2^2} - (\hat{a}_0^1 \cdot \hat{d}_0) x_1, \\
0 &= ((\hat{a}_1^0 + \hat{a}_1^1) \cdot \hat{n}) \sqrt{1 - x_0^2 - x_2^2} \sqrt{1 - x_1^2 - x_2^2} \\
&- \ (\hat{a}_0^0 \cdot \hat{d}_0) \sqrt{1 - x_0^2 - x_2^2} x_2 - (\hat{a}_1^1 \cdot \hat{d}_1) \sqrt{1 - x_1^2 - x_2^2} x_2.
\end{align*}
\]

The values of \( x_0, x_1 \) and \( x_2 \) that maximize \( P_U \), denoted by \( x_0^\text{max}, x_1^\text{max} \) and \( x_2^\text{max} \), are easily seen to be those given by Eq. (2.17). These define \( \vec{r}^\text{max} \) through Eq. (2.16).

If \( |\vec{r}^\text{max}| \leq 1 \), then it corresponds to the optimal density operator. If \( |\vec{r}^\text{max}| > 1 \), then there is no extremum of \( P_U \) inside the Bloch ball and the optimal density operator must be represented by a point on the boundary of the ball. Such a point corresponds to a
If $f$ is seen to the dot easily, the value of $a_0$ must be represented...
pure state. Consequently there is no freedom in the convex decomposition Alice realizes, and all that she must decide is what state to tell Bob to test for. If she tells him $|\psi^0_k\rangle$ when she wishes to unveil a bit value of 0 and $|\psi^1_k\rangle$ when she wishes to unveil a bit value of 1, then in terms of Bloch vectors, her probability of unveiling the bit of her choosing is

$$P_U = \frac{1}{4} \left( 1 + \hat{r} \cdot \hat{a}^0_k \right) + \frac{1}{4} \left( 1 + \hat{r} \cdot \hat{a}^1_{k'} \right)$$

$$= \frac{1}{2} + \frac{1}{4} \hat{r} \cdot (\hat{a}^0_k + \hat{a}^1_{k'}) ,$$

where we write $\hat{r}$ to emphasize that we are varying over pure density operators. The vector $\hat{r} = \frac{\hat{a}^0_k + \hat{a}^1_{k'}}{|\hat{a}^0_k + \hat{a}^1_{k'}|}$ clearly maximizes $P_U$. In our notational convention, $\hat{a}^0_k$ and $\hat{a}^1_{k'}$ are the closest pair of Bloch vectors from the two sets, so Alice should choose $k = k' = 1$. It follows that the optimal density operator is represented by the Bloch vector defined in Eq. (2.15).

Note that it may occur that $\hat{a}^0_k$ and $\hat{a}^1_{k'}$ are as close to one another as $\hat{a}^0_{k'}$ and $\hat{a}^1_k$, that is, it may occur that there is no unique 'closest' pair of Bloch vectors. However, in this case one will not find $|\hat{r}^{\text{max}}| > 1$. The reason is as follows. If one did find $|\hat{r}^{\text{max}}| > 1$, then the optimal $\hat{r}$ would have to be a pure state. However, since the pure states associated with the Bloch vectors $\frac{\hat{a}^0_k + \hat{a}^1_{k'}}{|\hat{a}^0_k + \hat{a}^1_{k'}|}$ and $\frac{\hat{a}^0_{k'} + \hat{a}^1_k}{|\hat{a}^0_{k'} + \hat{a}^1_k|}$ would yield the same $P_U$, any mixture of these would also yield this $P_U$. This in turn would imply that there existed a solution with $|\hat{r}^{\text{max}}| < 1$. □

**Proof for case 2.1.** Since $\hat{a}^0_k$, $\hat{a}^0_{k'}$, $\hat{a}^1_k$ and $\hat{a}^1_{k'}$ all lie in a plane, $\hat{a}^b_k \cdot \hat{n}$ is independent of $b$ and $k$. In this case, we find $x_0^{\text{max}} = \hat{a}^1_k \cdot \hat{d}^k$, $x_1^{\text{max}} = \hat{a}^0_{k'} \cdot \hat{d}^k$ and $x_2^{\text{max}} = \hat{a}^0_k \cdot \hat{n}$. That this corresponds to the point of intersection can be verified from the parametric equations for the lines containing the two chords. □

**Proof for case 2.2.** If the chord defined by $\hat{a}^b_k$ and $\hat{a}^b_{k'}$ passes through the $\hat{n}$ axis,
then it must lie in the plane of \( \hat{d}_1 \) and \( \hat{n} \), so that \( \hat{a}^b_k \cdot \hat{d}^\perp_1 = 0 \). It follows that \( x^\max_0 = x^\max_1 = 0 \), and thus \( \hat{r}^\max = x^\max_2 \hat{n} \). Since \( |x^\max_2| \leq 1 \), we know that \( |\hat{r}^\max| \leq 1 \), so that \( \hat{r}^\opt = \hat{r}^\max = x^\max_2 \hat{n} \). □

**Proof for case 2.3.** The case being considered corresponds to \( \hat{n} \cdot (\hat{a}^0_k + \hat{a}^1_k) = 0 \). We must consider the two possibilities \( |\hat{r}^\max| \leq 1 \) and \( |\hat{r}^\max| > 1 \). In the former, \( \hat{r}^\opt = \hat{r}^\max \), while in the latter \( \hat{r}^\opt = \frac{\hat{a}^0_k + \hat{a}^1_k}{|\hat{a}^0_k + \hat{a}^1_k|} \). Either way, the condition \( \hat{n} \cdot (\hat{a}^0_k + \hat{a}^1_k) = 0 \) implies that \( \hat{r}^\opt \cdot \hat{n} = 0 \). □
Appendix C

Proof of Lemma 1 of chapter 3

Proof of Lemma 1. The density operators for qubits can be represented by vectors on the Bloch sphere. If \( \rho \) and \( \sigma \) are represented by vectors \( \vec{r} \) and \( \vec{s} \), then in terms of these, the trace distance and fidelity squared can be written as [7][52]

\[
D(\rho, \sigma) = \frac{1}{2} |\vec{r} - \vec{s}|,
\]

\[
F(\rho, \sigma)^2 = \frac{1}{2} \left( 1 + \vec{r} \cdot \vec{s} + \sqrt{(1 - |\vec{r}|^2)(1 - |\vec{s}|^2)} \right).
\]

Defining \( r = |\vec{r}|, s = |\vec{s}| \) and \( \cos \phi = \vec{r} \cdot \vec{s}/rs \), we have

\[
D + F^2 = \frac{1}{2} \sqrt{r^2 + s^2 - 2rs \cos \phi}
\]

\[
+ \frac{1}{2} \left( 1 + rs \cos \phi + \sqrt{(1 - r^2)(1 - s^2)} \right).
\]

This is minimized for \( \phi = 0 \). Moreover, assuming (arbitrarily) that \( r \geq s \), we have \( \sqrt{r^2 + s^2 - 2rs} = r - s \) and \( \sqrt{(1 - r^2)(1 - s^2)} \geq (1 - r)(1 + s) \). Together, these facts imply \( D(\rho, \sigma) + F(\rho, \sigma)^2 \geq 1 \). \( \square \)
Appendix D

Some remarks on the fragmentation of Bose-Einstein condensates

It is customary to approximate the $N$-body ground state of a system of spinless bosons by the Hartree-Fock state

$$|N\rangle_{\phi_0} = \frac{\left(\int d^3 r \phi_0(r) \hat{\psi}^+(r)\right)^N}{\sqrt{N!}} |\text{vac}\rangle,$$

where $\phi_0(r)$ is a normalized single particle wavefunction. This describes an accumulation of $N$ particles in the wavefunction $\phi_0(r)$. One can, however, also consider states of the form

$$|N_1\rangle_{\phi_1} |N_2\rangle_{\phi_2} = \frac{\left(\int d^3 r \phi_1(r) \hat{\psi}^+(r)\right)^{N_1}}{\sqrt{N_1!}} \frac{\left(\int d^3 r \phi_2(r) \hat{\psi}^+(r)\right)^{N_2}}{\sqrt{N_2!}} |\text{vac}\rangle,$$

where $\phi_1(r)$ and $\phi_2(r)$ are normalized and orthogonal single-particle wavefunctions, and where $N_1 + N_2 = N$. Such a state describes an accumulation of $N_1$ particles in the wavefunction $\phi_1(r)$ and $N_2$ particles in $\phi_2(r)$. We distinguish states of the form $|N\rangle_{\phi_0}$ from those of the form $|N_1\rangle_{\phi_1} |N_2\rangle_{\phi_2}$ by designating the first as ‘single condensates’ and the second as ‘dual condensates’. It is evident that one can also introduce states describing the accumulation of particles in an arbitrary number of orthogonal single-particle wave-
functions. Such states can be referred to collectively as 'fragmented condensates' [22]. In this appendix, we show how a non-uniform trap potential can encourage fragmentation. In particular, we demonstrate that in a double minimum potential a dual condensate can have an expectation value of the energy smaller than that of a single condensate, and therefore can constitute a better approximation to the fully interacting ground state and a better starting point for treatments beyond Hartree-Fock.

This result may be surprising to some and obvious to others. Specifically, it seems remarkable in light of Nozières' argument against fragmentation of condensates [22]. On the other hand, it seems natural to describe bosons in well-separated traps by a product of single condensate states for each trap; for two traps, such a product state would be a dual condensate wherein each of $\phi_1(r)$ and $\phi_2(r)$ is centered in only one of the traps. Indeed, this has been assumed implicitly in the literature when discussing the interference of condensates [101]. Our analysis justifies this intuition and specifies the circumstances under which Nozières' argument is inapplicable.

D.1 Desiderata for fragmentation

We consider a two-particle interaction that is local and completely repulsive: $V(r, r') = g\delta(r - r')$. The interaction strength is given by $g = 4\pi a_{sc} \hbar^2/m$, where $a_{sc}$ is the s-wave scattering length, assumed to be positive, and where $m$ is the mass of the particle. For simplicity we restrict ourselves to wavefunctions $\phi_0(r)$, $\phi_1(r)$, and $\phi_2(r)$ that are real. Consider the expectation value of the energy for a single condensate $|N\rangle_{\phi_0}$.

$$E_n = N\epsilon(\phi_0) + \frac{1}{2} g N(N - 1) \int \phi^*_0(r) d^3r,$$  \hspace{1cm} (D.2)
where \( \epsilon(\phi) = \int \phi(r) \left[ -\frac{\hbar^2}{2m} \nabla^2 + U(r) \right] \phi(r) d^3r \) is the single particle energy associated with \( \phi(r) \), and \( U(r) \) is the trap potential. For the dual condensate \( |N_1\rangle_{\phi_1} |N_2\rangle_{\phi_2} \),

\[
E_i = N_1\epsilon(\phi_1) + N_2\epsilon(\phi_2) + \frac{1}{2} g N_1(N_1 - 1) \int \phi_1^4(r) d^3r \\
+ \frac{1}{2} g N_2(N_2 - 1) \int \phi_2^4(r) d^3r + 2g N_1 N_2 \int \phi_1^2(r) \phi_2^2(r) d^3r. \tag{D.3}
\]

If we assume that the particle densities are similar throughout the single and dual condensates, \( N_1 \phi_1^2(r) + N_2 \phi_2^2(r) \approx N \phi_0^2(r) \), then the pieces of the interaction energies that scale as \( N^2 \) are

\[
E_{i}^{\text{quad}} = \frac{1}{2} g N^2 \int \phi_0^4(r) d^3r \\
E_{d}^{\text{quad}} = \frac{1}{2} g N_1^2 \int \phi_1^4(r) d^3r + \frac{1}{2} g N_2^2 \int \phi_2^4(r) d^3r + 2g N_1 N_2 \int \phi_1^2(r) \phi_2^2(r) d^3r \approx \frac{1}{2} g N^2 \int \phi_0^4(r) d^3r + g N_1 N_2 \int \phi_1^2(r) \phi_2^2(r) d^3r. \tag{D.4}
\]

We can think of this in the following way: while the Hartree contributions to the interaction energy of the single and dual condensates are essentially equal, the interaction energy of the dual condensate also includes an exchange term, proportional to \( N_1 N_2 \), arising from symmetrization.

This extra exchange energy was identified by Nozières [22] and is the basis of his argument against fragmentation of the condensate, since in the limit of a macroscopic number of particles, \( E_{d}^{\text{quad}} \) exceeds \( E_{i}^{\text{quad}} \) by a macroscopic energy. However, this argument assumes that the wavefunctions have a similar spatial extent \( \phi_1^2(r) \approx \phi_2^2(r) \approx \phi_0^2(r) \). If instead one considers a dual condensate wherein \( \phi_1 \) and \( \phi_2 \) have little density overlap, then the exchange term may be small compared to other terms in (D.4) that are linear in \( N \), and we must consider the relative weights of all the terms.

The energies \( E_{d}^{\text{quad}} \) and \( E_{i}^{\text{quad}} \) overestimate the interaction energy since they incorporate a particle's interaction with itself. Thus, to obtain the proper interaction energy, we
must add to $E_{q}^{\text{quad}}$ a term linear in $N$

$$E_{q}^{\text{lin}} = -\frac{1}{2} gN \int \phi_{0}^{4}(r)d^{3}r.$$  \hspace{1cm} (D.5)

Similarly, we must add to $E_{d}^{\text{quad}}$ the linear term

$$E_{d}^{\text{lin}} = -\frac{1}{2} gN_{1} \int \phi_{1}^{4}(r)d^{3}r - \frac{1}{2} gN_{2} \int \phi_{2}^{4}(r)d^{3}r.$$  \hspace{1cm} (D.6)

If $\phi_{1}$ and $\phi_{2}$ are more localized than $\phi_{0}$, then $\int \phi_{1,2}^{4}(r)d^{3}r > \int \phi_{0}^{4}(r)d^{3}r$. It follows that $E_{d}^{\text{lin}} - E_{s}^{\text{lin}} < 0$. Thus, the linear piece of the interaction energy favors the dual condensate.

Admittedly, it will cost more single particle energy to place particles in localized wavefunctions like $\phi_{1}$ and $\phi_{2}$ than in $\phi_{0}$, so the single particle energy favors the single condensate. Thus we see that there is a competition between the interaction energy benefit that may arise from separating the bosons, and the single particle energy cost of establishing this separation. The role of the trap potential in fragmentation is now clear: for a non-uniform potential, one can construct wavefunctions that are confined to the valleys of the potential and which have little density overlap without a large cost of single particle energy. A non-uniform potential therefore encourages spatial fragmentation.

## D.2 Fragmentation in a double well potential

We now turn to a simple model of the condensate in a potential well that is symmetric along each Cartesian axis, but which along one axis ($x$) exhibits a double minimum. We wish to consider which of the single or dual condensate is energetically favored as a function of the strength of the central barrier of the potential. As is customary, one minimizes the energy of the single condensate with respect to variations in $\phi_{0}$ to obtain a non-linear Schrödinger equation (NLSE) for $\phi_{0}$. Due to the symmetry of the potential, we expect that the energetically favored dual condensate will have the particles distributed...
equally between wavefunctions that are mirror images of one another across \( x = 0 \), that is, \( \phi_1(-x,y,z) = \phi_2(x,y,z) \) and \( N_1 = N_2 = N/2 \). Assuming a dual condensate of this form, we can minimize its energy with respect to variations in \( \phi_1 \) and \( \phi_2 \) to obtain two coupled NLSEs for \( \phi_1 \) and \( \phi_2 \).

Let us first consider the case of an infinitely strong barrier; all wavefunctions will then have zero amplitude at the center of the barrier. The single condensate that minimizes the expectation value of the energy has a degeneracy associated with the different possible symmetries of the wavefunction across the barrier. Let us denote the symmetric solution of the single condensate NLSE as \( \phi_s \) and the antisymmetric solution as \( \phi_a \). We can then construct two wavefunctions \( \phi_l = 2^{-1/2}(\phi_s + \phi_a) \) and \( \phi_r = 2^{-1/2}(\phi_s - \phi_a) \) that are confined respectively to the left \( (x < 0) \) and right \( (x > 0) \) of the barrier, and which have the same single particle energy as \( \phi_s \).

In the single condensate \( |N\rangle_{\phi_s} \), the magnitude of the interaction energy is \( \frac{1}{2}gN(N-1) \int \phi_s^2(r)d^3r \). This can be understood as follows: there are \( N \) particles interacting with \( N-1 \) others with an interaction strength of \( g \int \phi_s^2(r)d^3r \), and the factor of \( 1/2 \) is due to over-counting. Now consider the particular dual condensate that is of the form \( |N/2\rangle_{\phi_s} |N/2\rangle_{\phi_a} \), noting that this state is not necessarily the solution of the dual condensate variational problem. The interaction energy of this state originates solely from the interaction of particles with others in the same wavefunction, since the density overlap of the two wavefunctions, \( \int \phi_l^2(r)\phi_r^2(r)d^3r \), is zero. Particles in this dual condensate interact twice as intensely with one another than in the single condensate since \( \int \phi_l^2(r)d^3r = \int \phi_r^2(r)d^3r = 2 \int \phi_s^2(r)d^3r \). However, each of the \( N \) particles sees only \( N/2 - 1 \) others rather than \( N-1 \) others. Including the over-counting factor of \( 1/2 \), the total interaction energy of this dual condensate is \( \frac{1}{2}gN(N-2) \int \phi_s^4(r)d^3r \). This interaction energy is clearly less than that of the single condensate. Since the single particle energies are the same for the two states, it follows that the dual condensate \( |N/2\rangle_{\phi} |N/2\rangle_{\phi} \) is energetically favored overall. Further, the dual condensate that is obtained from solving
the variational problem may have an energy that is lower still.
Appendix E

Proof of Theorem 1 of chapter 5

It will be assumed throughout that the distinguished factorization is bi-partite, and the two factor spaces are denoted by $\mathcal{H}^A$ and $\mathcal{H}^B$. All references to product decompositions are to be understood as product decompositions with respect to this factorization. We say that a product decomposition $\{(c_k, |x_k^A\rangle \otimes |\phi_k^B\rangle)\}_{k=1}^m$ is $A$-orthogonal ($B$-orthogonal) if the set of vectors $\{|x_k^A\rangle\}_{k=1}^m$ ($|\phi_k^B\rangle\}_{k=1}^m$) is orthogonal. A bi-orthogonal decomposition (also called a Schmidt decomposition) is one that is both $A$-orthogonal and $B$-orthogonal. We shall make use of several well-known properties of bi-orthogonal decompositions [42]. Finally, we remind the reader that $S_{|\psi\rangle}(D)$ denotes the IU entropy of $|\psi\rangle$ for the decomposition $D$, which is defined by Eq. (5.2).

Theorem 1 follows from two lemmas:

**Lemma E.1** For any vector $|\psi\rangle$, if $D$ is an arbitrary product decomposition of $|\psi\rangle$, then there always exists an $A$-orthogonal decomposition of $|\psi\rangle$, $D_{A\text{-orth}}$, such that

$$S_{|\psi\rangle}(D_{A\text{-orth}}) \leq S_{|\psi\rangle}(D).$$

**Lemma E.2** For any vector $|\psi\rangle$, if $D_{A\text{-orth}}$ is any $A$-orthogonal decomposition of $|\psi\rangle$. 

161
and $D_{\text{bi-orth}}$ is any bi-orthogonal decomposition of $|\psi\rangle$, then

$$S_{|\psi\rangle}(D_{\text{bi-orth}}) \leq S_{|\psi\rangle}(D_{A-\text{orth}}).$$

Together these imply that for any vector $|\psi\rangle$, if $D$ is an arbitrary product decomposition of $|\psi\rangle$, and $D_{\text{bi-orth}}$ is any bi-orthogonal decomposition of $|\psi\rangle$, then

$$S_{|\psi\rangle}(D_{\text{bi-orth}}) \leq S_{|\psi\rangle}(D),$$

which is simply theorem 1.

The task at hand is therefore to prove lemmas E.1 and E.2. We begin by reviewing a partial ordering relation among probability distributions, namely that of majorization [102], which has recently seen application in the study of entanglement purification [103]. Suppose $p \equiv (p_1, p_2, ..., p_m)$ and $q \equiv (q_1, q_2, ..., q_m)$ are two $m$-element probability distributions. By definition, $p$ majorizes $q$ if for every $l$ in the range $\{1, ..., m\}$,

$$\sum_{k=1}^{l} p_k^l \geq \sum_{k=1}^{l} q_k^l,$$

where $p_k^l$ indicates the $k$th largest element of $p$, so that $p_1^l \geq p_2^l \geq ... \geq p_m^l$.

The notion of majorization is important in the present investigation because of the following well-known result (Theorem II.3.1 of Bhatia [102]): The following two conditions are equivalent

(i) $p$ majorizes $q$.

(ii) $\sum_{k=1}^{m} f(p_k) \leq \sum_{k=1}^{m} f(q_k)$ for all concave functions $f$.

Since $-x \log x$ is a concave function of $x$, it follows that $H(p) \leq H(q)$ if and only if $p$ majorizes $q$, where $H(p)$ is the Shannon entropy of a probability distribution $p$, defined
in Eq. (5.1). Now consider two decompositions of a state vector, \( D = \{ |e_k, \phi_k \rangle \}_{k=1}^m \) and \( D' = \{ |e'_k, \phi'_k \rangle \}_{k=1}^{m'} \). Although these may have different cardinalities, they can be associated with probability distributions of equal cardinality by simply adding zeroes. Specifically, if \( m \geq m' \), then \( D \) is associated with the distribution \( p_k = |c_k|^2 \) for \( k \in \{1, ..., m\} \) and \( D' \) is associated with the distribution \( q_k = |c'_k|^2 \) for \( k \in \{1, ..., m'\} \) and \( q_k = 0 \) for \( k \in \{m' + 1, ..., m\} \). Since the entropy of \( |\psi\rangle \) for the decomposition \( D(D') \) is simply the Shannon entropy of \( p(q) \), it follows that \( S_{|\psi\rangle}(D) \leq S_{|\psi\rangle}(D') \) if \( p \) majorizes \( q \).

In order to facilitate the proof of lemma E.1, we set out two minor lemmas.

**Lemma E.3** Consider two probability distributions \( p \equiv (p_1, p_2, ..., p_m) \) and \( q \equiv (q_1, q_2, ..., q_m) \). If for every \( l \) in the range \( \{1, ..., m\} \),

\[
\sum_{k=1}^{l} p_k \geq \sum_{k=1}^{l} q_k,
\]

then \( p \) majorizes \( q \).

**Proof.** This result follows from the definition of majorization and the fact that

\[
\sum_{k=1}^{l} p_k^l \geq \sum_{k=1}^{l} p_k
\]

for every \( l \) in the range \( \{1, ..., m\} \). This inequality is obviously true since the \( l \)-element subset of \( p \) with the largest sum must be the subset containing the \( l \) largest elements of \( p \). \( \square \)

For the second minor lemma, we make use of the following notational conventions: \( P_S \) denotes the projector onto the subspace \( S \), and \( 'P_S < P_{S'}' \) denotes that \( S \) is a proper subspace of \( S' \).

**Lemma E.4** If \( P_S \leq P_{S'} \) then \( \langle \psi | P_S | \psi \rangle \leq \langle \psi | P_{S'} | \psi \rangle \).
Proof. If \( P_S = P_{S'} \), then the inequality is saturated. Otherwise, \( P_S < P_{S'} \), and there exists a projector \( P_T \) such that \( P_S + P_T = P_{S'} \). The desired inequality follows from the positivity of \( \langle \psi | P_T | \psi \rangle \). □

We are now in a position to prove lemma E.1.

Proof of lemma E.1. An arbitrary product decomposition has the form \( D = \prod_k \langle \phi_k^A \rangle \otimes \langle \chi_k^B \rangle \), where the lists of vectors \( \{ \langle \phi_k^A \rangle \}_{k=1}^m \) and \( \{ \langle \chi_k^B \rangle \}_{k=1}^m \) are not necessarily orthogonal nor even linearly independent (although the list of vectors \( \{ \langle \phi_k^A \rangle \otimes \langle \chi_k^B \rangle \}_{k=1}^m \) is orthogonal). The decomposition \( D \) defines an \( m \)-element probability distribution \( q = \{ q_1, q_2, \ldots, q_m \} \), where \( q_k \equiv |d_k|^2 \). As before, let \( q_k^i \) denote the \( k \)th largest element of \( q \), and let \( \langle \phi_k^A \rangle \) and \( \langle \chi_k^A \rangle \) denote the vectors associated with \( q_k^i \).

Now, identify every vector in the list \( \{ \langle \phi_k^A \rangle \}_{k=1}^m \) that cannot be obtained as a linear combination of vectors with lower indices from this list. Suppose there are a number \( m' \) of such vectors, corresponding to a particular subset \( S \) of the indices \( \{ 1, 2, \ldots, m \} \), so that the set of vectors is denoted by \( \{ \langle \phi_k^A \rangle \}_{k \in S} \). By definition, this is a linearly independent set. The remaining vectors are denoted by \( \{ \langle \phi_k^A \rangle \}_{k \in \bar{S}} \), where \( \bar{S} \) is the set of indices that remain after removing the elements of \( S \) from \( \{ 1, 2, \ldots, m \} \). Obviously each element of \( \{ \langle \phi_k^A \rangle \}_{k \in \bar{S}} \) can be written as a linear combination of the elements of \( \{ \langle \phi_k^A \rangle \}_{k' \in S, k' < k} \). Finally, for future reference, we define \( g(k) \) as the number of indices \( k' \) in \( S \) such that \( k' \leq k \). It is clear from the definition of \( S \) that \( g(k) \leq k \).

Let \( \{ \langle \mu_j^A \rangle \}_{j=1}^{m'} \) be the ordered set of orthogonal vectors that are obtained by applying the Gram-Schmidt orthogonalization procedure to \( \{ \langle \phi_k^A \rangle \}_{k \in S} \), in order of ascending \( k \). This new set yields an \( A \)-orthogonal decomposition of \( |\psi\rangle \), \( D_{A-orth} = \{ \langle c_j | \mu_j^A \rangle \otimes |\nu_j^B\rangle \}_{j=1}^{m'} \), where \( |\nu_j^B\rangle = \langle \mu_j^A |\psi\rangle /c_j \) and \( c_j = |\langle \mu_j^A |\psi\rangle| \). It also defines an \( m' \)-element probability distribution \( p = (p_1, p_2, \ldots, p_m) \) where \( p_j \equiv |c_j|^2 \) for \( j \) in the range \( \{ 1, \ldots, m' \} \), and \( p_j \equiv 0 \) for \( j \) in the range \( \{ m' + 1, \ldots, m \} \).

Let \( P_{\phi}^A \) denote the projector onto the ray spanned by \( |\phi^A\rangle \) and for convenience define \( P_{\mu_j}^A \equiv P_{null} \) for \( j \) in the range \( \{ m', \ldots, m \} \). The nature of the Gram-Schmidt orthog-
A formalization procedure ensures that for every $k \in \mathcal{S}$, $|\phi^A_k\rangle = \sum_{j=1}^{g(k)} f_j |\mu^A_j\rangle$ for some set of complex amplitudes $\{f_j\}_{j=1}^{g(k)}$. Thus, $\langle \sum_{j=1}^{g(k)} P^A_{\mu_j} |\phi^A_k\rangle = |\phi^A_k\rangle$, or equivalently, $\sum_{j=1}^{g(k)} P^A_{\mu_j} \geq P^A_{\phi_k}$. Since $g(k) \leq k$, this is trivially extended to $\sum_{j=1}^{k} P^A_{\mu_j} \geq P^A_{\phi_k}$. Moreover, if $k \in \tilde{\mathcal{S}}$, then $|\phi^A_k\rangle$ can be written as a linear combination of the elements of $\{|\phi^A_{k'}\rangle\}_{k' \in S, k' < k}$, so that $|\phi^A_k\rangle = \sum_{j=1}^{g(h(k))} f_j |\mu^A_j\rangle$ for some set of complex amplitudes $\{f_j\}_{j=1}^{g(h(k))}$, where $h(k) = \max_{k' \in S, k' < k} k'$. It follows that $\sum_{j=1}^{g(h(k))} P^A_{\mu_j} \geq P^A_{\phi_k}$ for all $k \in \tilde{\mathcal{S}}$.

Since $g(h(k)) < k$, this is trivially extended to $\sum_{j=1}^{k} P^A_{\mu_j} \geq P^A_{\phi_k}$. It follows therefore that for every $k$ in the range $\{1, \ldots, m\}$ we have $\sum_{j=1}^{k} P^A_{\mu_j} \geq P^A_{\phi_k}$. Next, since $I^B \geq P^B_{\chi_1}$, we can infer that $\sum_{j=1}^{k} P^A_{\mu_j} \otimes I^B \geq P^A_{\phi_k} \otimes P^B_{\chi_1}$, and by the orthogonality of the projectors in the set $\{P^A_{\phi_k} \otimes P^B_{\chi_1}\}_{i=1}^k$, we conclude that $\sum_{j=1}^{k} P^A_{\mu_j} \otimes I^B \geq \sum_{i=1}^{k} P^A_{\phi_i} \otimes P^B_{\chi_1}$ for every $k$ in the range $\{1, \ldots, m\}$.

Now we note that the probability distributions $q$ and $p$ are related to the projectors by $q^i = \langle \psi | P^A_{\phi_i} \otimes P^B_{\chi_1} | \psi \rangle$ and $p = \langle \psi | P^A_{\mu_j} \otimes I^B | \psi \rangle$. From the inequality derived above together with lemma E.4, we find that $\sum_{j=1}^{k} p_j \geq \sum_{i=1}^{k} q^i$ for every $k$ in the range $\{1, \ldots, m\}$. By lemma E.3, it follows that $p$ majorizes $q$. □

Finally, we prove lemma E.2.

**Proof of lemma E.2.** An arbitrary $A$-orthogonal decomposition of $|\psi\rangle$ has the form $D_{A\text{-orth}} = \{(c_j, |\mu^A_j\rangle \otimes |\nu^B_j\rangle)\}_{j=1}^m$, where the vectors $\{|\mu^A_j\rangle\}_{j=1}^m$ are orthogonal, but $\{|\nu^B_j\rangle\}_{j=1}^m$ need not be orthogonal nor even linearly independent. A bi-orthogonal decomposition of $|\psi\rangle$ has the form $D_{bi\text{-orth}} = \{(\tilde{c}_j, |\tilde{\mu}^A_j\rangle \otimes |\tilde{\nu}^B_j\rangle)\}_{j=1}^m$, where both the vectors $\{|\tilde{\mu}^A_j\rangle\}_{j=1}^m$ and $\{|\tilde{\nu}^A_j\rangle\}_{j=1}^m$ form orthogonal sets. The probability distributions associated with each decomposition are $(|c_1|^2, |c_2|^2, \ldots, |c_m|^2)$ and $(|\tilde{c}_1|^2, |\tilde{c}_2|^2, \ldots, |\tilde{c}_m|^2)$, respectively; even if there is more than one bi-orthogonal decomposition for a particular state vector, these do not differ in their coefficients. For ease of comparison of these distributions, we add zeroes until the number of elements in each is equal to the dimensionality $d$ of the Hilbert space $\mathcal{H}^A$. Denote the resulting distributions by $p$ and $\tilde{p}$ respectively. We establish that $S_{|\psi\rangle}(D_{bi\text{-orth}}) \leq S_{|\psi\rangle}(D_{A\text{-orth}})$ by showing that $\tilde{p}$ majorizes $p$. 


To begin, we express the probabilities as expectation values of projectors. We introduce an arbitrary orthogonal set of vectors $\{\vert \mu_j^A \rangle \}_{j=m+1}^d$ which together with $\{\vert \mu_j^A \rangle \}_{j=1}^m$ form an orthogonal basis for the Hilbert space $\mathcal{H}^A$, and similarly for $\{\vert \tilde{\mu}_j^A \rangle \}_{j=1}^m$. Then, we have for all $j$ in the range $\{1, \ldots, d\}$,

\[ p_j = \text{Tr}_A (\rho^A P^A_{\mu_j}), \text{ and} \]
\[ \tilde{p}_j = \text{Tr}_A (\rho^A P^A_{\tilde{\mu}_j}). \]

Let the unitary operator that transforms the elements of $\{\vert \tilde{\mu}_j^A \rangle \}_{j=1}^d$ to the elements of $\{\vert \mu_j^A \rangle \}_{j=1}^d$ be denoted by $U^A$, so that

\[ \vert \mu_j^A \rangle = U^A \vert \tilde{\mu}_j^A \rangle. \]

It follows that

\[ p_j = \text{Tr}_A (\rho^A U^A P^A_{\tilde{\mu}_j} U^A) \]
\[ = \text{Tr}_A (U^A \rho^A U^A P^A_{\tilde{\mu}_j} U^A), \]

where in the last step we have used the cyclic property of the trace. What distinguishes the bi-orthogonal decomposition from other $A$-orthogonal decompositions is that the projectors $\{P^A_{\mu_k}\}_{k=1}^d$ diagonalize $\rho^A$,

\[ \rho^A = \sum_{k=1}^d \tilde{\rho}_k F^A_{\mu_k}. \]

Plugging this form of $\rho^A$ into the expression for $p_j$, we obtain

\[ p_j = \sum_{k=1}^d |U^A_{jk}|^2 \tilde{\rho}_k, \]
where $U_{jk}^A = \langle \bar{\mu}_j | U^A | \bar{\mu}_k \rangle$. By the unitarity of $U^A$, we find that $\sum_j |U_{jk}^A|^2 = \langle \bar{\mu}_k | U^{A\dagger} U^A | \bar{\mu}_k \rangle = 1$, and $\sum_k |U_{jk}^A|^2 = \langle \bar{\mu}_j | U^A U^{A\dagger} | \bar{\mu}_j \rangle = 1$. Thus, the transition matrix between the probability distributions $\bar{\mathbf{p}}$ and $\mathbf{p}$ is doubly stochastic, from which it follows by a well-known result (Theorem II.1.9 of Bhatia [102]) that $\bar{\mathbf{p}}$ majorizes $\mathbf{p}$. □
Bibliography


[27] To add drama to the story, one can imagine that the whole measurement takes place inside a box which also contains a cat, and that obtaining a particular outcome triggers a chain of events which leads to the untimely death of the cat. In this case, the orthodox approach would fail to predict that the cat had either the property of being alive or the property of being dead [2].


[29] This use of the term ‘modal interpretation’ is consistent with that found in Clifton [30], but differs from that of van Fraassen [31] for whom a modal interpretation need not be realist. We restrict the scope of the term here for convenience.


[49] In this investigation, we consider only BC protocols that can be implemented between parties who each have only a single laboratory that is localized in space. Kent has shown [50] that unconditionally secure BC can be achieved if one relaxes this constraint, for instance, if both parties have a pair of laboratories separated by a distance $L$ (so that there are four laboratories in all), each of which can be verified to be a distance $d$ to one of the other party's laboratories, with $d \ll L$. The security stems from the constraint imposed by special relativity on the speed of communications between a party's two laboratories. Unfortunately, the protocol requires a channel capacity that increases exponentially with the duration of the holding phase.


[51] The degree of concealment quantifies the extent to which the protocol prevents Bob from gaining information about Alice's commitment. This is the standard notion of security against Bob in BC. Nonetheless, there are cryptographic tasks (such as coin tossing) wherein it is useful to consider a different type of security against Bob, namely, cheat detection. A protocol with this type of security ensures that if Bob gains any information about Alice's commitment then Alice has some finite probability of detecting that he has done so. We shall not consider this type of security here, however, see Ref. [15].


[53] Again, we are only considering protocols that can be implemented between localized parties, as discussed in Ref. [49]. It has been shown by Kent [54] that if one relaxes
this constraint, unconditionally secure coin tossing with arbitrarily small biases can be achieved.


[64] The term ‘double condensate’ has been used to denote two condensates of atoms of different internal spin states [61]. We use the term ‘dual condensate’ for two condensates that are only distinguished by the spatial wavefunctions of the atoms.

[66] see Ref. [59] for a justification of this choice.


[85] G. Bacciagaluppi and M. Hemmo, in Healey and Hellman [33], p. 95.


[87] P. Vermaas, in Dieks and Vermaas [32], p. 103.


This idea is due mainly to Chris Fuchs. The analogy to relativity is due to Jeffrey Bub. See Ref. [99].

