Emergence of a classical world from within quantum theory

by

David Poulin

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics

Waterloo, Ontario, Canada, 2004
© David Poulin 2004
Author’s declaration

I hereby declare that I am the sole author of this thesis.

I authorize the University of Waterloo to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize the University of Waterloo to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.
Thesis Committee

This thesis has been evaluated, approved without modifications, and nominated for the Pearson medal on November 26th of the year 2004 by a jury composed of the following supervisors and examiners:

- William B. Anderson, Examination Chair
  Department of Chemical Engineering, University of Waterloo

- Artur Ekert, External Examiner
  Department of Applied Mathematics & Theoretical Physics, Cambridge University

- Raymond Laflamme, Supervisor
  Department of Physics, University of Waterloo

- Robert Mann, Member of Committee
  Department of Physics, University of Waterloo

- Michele Mosca, Internal-External Examiner
  Combinatorics & Optimization Department, University of Waterloo

- Lee Smolin, Member of Committee
  Department of Physics, University of Waterloo
Abstract

The starting point of this dissertation is that a quantum state represents the observer’s knowledge about the system of interest. As it has been pointed out several times by the opponents of this epistemic interpretation, it is difficult to reconcile this point of view with our common notion of “physical reality”, which exists independently of our monitoring, and can be discovered without disturbance. Indeed, if quantum theory is correct, it should apply to classical systems — including measurement devices — as well as to any other system.

In this dissertation, we will study the quantum mechanisms responsible for our perception of the world and demonstrate how they lead to the emergence of an operational objective reality from within quantum theory: several observers gathering information through these mechanisms will arrive at a common consensus about the properties of the world.

The two mechanisms we study in great detail are the redundant proliferation of information in the environment and the direct measurement of a macroscopic observable. An example of the first mechanism is the photon environment which provides us with our visual data about the world. Several independent observers learning about their surroundings in this indirect fashion will agree on their findings. An example of the second mechanism is our tactile information: when the tip of our finger touches an object, it interacts collectively with a very large number of molecules. Again, under realistic assumptions, this type of information acquisition will lead to a classical perception of the world.

Key words: Quantum-classical transition, Interpretation of quantum theory, Decoherence, Macroscopic observables, Weak measurements, Ensemble measurements, Nuclear magnetic resonance quantum information processing, Quantum information.
Résumé

Le point de départ de la présente dissertation est qu’un état quantique représente la connaissance d’un observateur par rapport au système à l’étude. Comme l’ont fait valloir les principaux opposants à cette interprétation dite épistémique de la théorie quantique, il est difficile de réconcilier ce point de vue avec notre notion commune de « réalité physique », réalité qui existe de façon indépendante de l’observation et qui peut être découverte sans être perturbée. En effet, si nous admettons que la théorie quantique est correcte, alors elle doit convenir à tous les systèmes physiques, aussi bien classiques que quantiques, dont en particulier les appareils de mesure.

Dans cette dissertation, nous présentons une étude détaillée des principaux mécanismes quantiques à l’aide desquels nous percevons notre univers. Nous démontrons comment une réalité objective peut émerger de ces mécanismes de façon opérationnelle: divers observateurs indépendants recueillant de l’information à l’aide de ces mécanismes arriverons à un consensus commun sur les propriétés de notre univers.

Nous identifions deux types de mécanismes responsables pour notre perception du monde: l’acquisition indirecte d’information par le billais de la prolifération d’information dans l’environnement et la mesure directe d’une quantité macroscopique. À titre d’exemple du premier mécanisme, citons l’environnement de photons responsable de toutes nos données visuelles. Plusieurs observateurs indépendants recueillant cette information visuelle arrivent toujours à un consensus sur les propriétés du monde qui les entourent.

Le second mécanisme peut décrire par exemple toute l’information tactile que nous recevons: lorsque la pointe de notre doigt touche un objet, elle interagit de façon collective avec un très grand nombre de molécules. Encore une fois, ce type d’acquisition d’information nous conduit à une perception classique de notre univers.

Mots clés: Transition quantique-classique, Interprétation de la théorie quantique, Détocohérence, Observables macroscopiques, Mesures faibles, Mesures d’ensemble, Manipulation d’information quantique par résonance magnétique nucléaire, Information quantique.
Contents

1 Motivation

1.0.1 The epistemic view ................................................. 2
1.0.2 Distinction between quantum and classical ...................... 3
1.0.3 Two questions ..................................................... 5
1.0.4 Our proposal .................................................... 6
1.1 Outline of the dissertation ........................................... 8
1.2 Additional information for the examiners of this thesis .......... 9

2 Environment as a witness ............................................. 13

2.1 Introduction .......................................................... 13
2.2 Objectivity: what is the problem? .................................. 15
2.3 Definitions and conventions ........................................ 19
2.4 Information ............................................................ 20
   2.4.1 Correlations between system and environment .............. 22
   2.4.2 Redundancy of information in the environment ............. 24
   2.4.3 Fragments of the environment and elementary subsystems .. 24
2.5 Consequences of redundancy ...................................... 26
2.6 Quantum Darwinism: Dynamical emergence of objectivity ...... 33
   2.6.1 Dynamics of Quantum Darwinism and decoherence ........... 34
   2.6.2 Decoherence: the focus on the system ........................ 36
   2.6.3 Perfect correlations ............................................. 36
   2.6.4 Imperfect correlations .......................................... 40
   2.6.5 Quantum Darwinism exemplified .............................. 42
2.7 Discussion ............................................................. 45
   2.7.1 Assumptions .................................................... 46
   2.7.2 The state $\rho^{SE}$ ............................................ 51
2.8 Summary and Conclusion ........................................... 54
3 Macroscopic observables

3.1 Overview ................................................................. 57
3.2 Definitions ............................................................... 59
  3.2.1 Method of types .................................................. 59
  3.2.2 Macroscopic observable ......................................... 61
  3.2.3 Coarse grained macroscopic POVMs ........................... 64
3.3 Type measurement on identically prepared systems ................. 66
  3.3.1 State disturbance ................................................ 67
  3.3.2 Gaussian smoothing ............................................. 71
  3.3.3 General smoothing .............................................. 72
  3.3.4 Mixed states .................................................... 75
3.4 Exchangeability ...................................................... 75
  3.4.1 Bulk tomography ................................................. 77
3.5 Classicality ........................................................... 79
3.6 NMR information processing ....................................... 85
3.7 Conclusion and open questions .................................... 89

4 Conclusions ............................................................. 93

A Environment as a witness: mathematical complement ............... 97

B Macroscopic observables: mathematical complement ............... 101
  B.1 Single molecule post-measurement state .......................... 101
  B.2 Conditional fidelity ............................................... 103

C Other work published during Ph.D. program .......................... 107
  C.1 Robust polarization-based quantum key distribution over collective-noise channel† .................................................. 107
  C.2 Exponential speed-up with a single bit of quantum information: Measuring the average fidelity decay† ........................................ 117
    C.2.1 Efficient algorithm ............................................ 121
    C.2.2 Entanglement .................................................. 122
    C.2.3 Quantum probe .............................................. 123
    C.2.4 Numerical study ............................................. 124
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.2.5</td>
<td>Conclusion</td>
<td>124</td>
</tr>
<tr>
<td>C.3</td>
<td>Estimation of the Local Density of States on a Quantum Computer*</td>
<td>127</td>
</tr>
<tr>
<td>C.4</td>
<td>Testing integrability with a single bit of quantum information*</td>
<td>137</td>
</tr>
<tr>
<td>C.4.1</td>
<td>Overview</td>
<td>138</td>
</tr>
<tr>
<td>C.4.2</td>
<td>Level distribution</td>
<td>139</td>
</tr>
<tr>
<td>C.4.3</td>
<td>Quantum algorithm</td>
<td>143</td>
</tr>
<tr>
<td>C.4.4</td>
<td>Numerical results</td>
<td>144</td>
</tr>
<tr>
<td>C.4.5</td>
<td>Conclusion</td>
<td>149</td>
</tr>
<tr>
<td>C.5</td>
<td>Compatibility of quantum states*</td>
<td>151</td>
</tr>
<tr>
<td>C.5.1</td>
<td>Measurements</td>
<td>157</td>
</tr>
<tr>
<td>C.5.2</td>
<td>Combining knowledge</td>
<td>158</td>
</tr>
<tr>
<td>C.5.3</td>
<td>Knowledge</td>
<td>159</td>
</tr>
<tr>
<td>C.6</td>
<td>Noiseless Subsystems for Collective Rotation Channels in Quantum Information Theory*</td>
<td>161</td>
</tr>
<tr>
<td>C.6.1</td>
<td>Introduction</td>
<td>162</td>
</tr>
<tr>
<td>C.6.2</td>
<td>Background</td>
<td>163</td>
</tr>
<tr>
<td>C.6.3</td>
<td>Collective Rotation Channels</td>
<td>166</td>
</tr>
<tr>
<td>C.6.4</td>
<td>Commutant Structure Theorem</td>
<td>169</td>
</tr>
<tr>
<td>C.6.5</td>
<td>Generalized Collective Rotation Channels</td>
<td>177</td>
</tr>
</tbody>
</table>
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Venn diagram for classical information.</td>
<td>23</td>
</tr>
<tr>
<td>2.2</td>
<td>Quantum Darwinism exemplified.</td>
<td>43</td>
</tr>
<tr>
<td>3.1</td>
<td>State disturbance for general smoothing.</td>
<td>74</td>
</tr>
<tr>
<td>C.1</td>
<td>Quantum circuit for the fidelity decay</td>
<td>122</td>
</tr>
<tr>
<td>C.2</td>
<td>Fidelity decay for the kicked top</td>
<td>125</td>
</tr>
<tr>
<td>C.3</td>
<td>Quantum circuit for the LDOS</td>
<td>131</td>
</tr>
<tr>
<td>C.4</td>
<td>Quantum circuit for evaluating the trace</td>
<td>143</td>
</tr>
<tr>
<td>C.5</td>
<td>Form factor for random matrices</td>
<td>145</td>
</tr>
<tr>
<td>C.6</td>
<td>Kicked top in regular regime</td>
<td>147</td>
</tr>
<tr>
<td>C.7</td>
<td>Kicked top in chaotic regime</td>
<td>147</td>
</tr>
<tr>
<td>C.8</td>
<td>Graphical representation of $\text{Tr}{\hat{F}}$</td>
<td>148</td>
</tr>
<tr>
<td>C.9</td>
<td>Transition from regular to chaotic</td>
<td>148</td>
</tr>
<tr>
<td>C.10</td>
<td>Structure of the commutant</td>
<td>170</td>
</tr>
</tbody>
</table>
Acknowledgments

Raymond Laflamme has been for the past three years a great research supervisor, a pretty good mountain bike partner, and a dear friend. Through the dynamical research environment he has built, by supporting my many travels, and by continually expressing his confidence in me, he has helped me to establish new and exciting research projects as well as to maintain old ones well alive. But most importantly, he always has the perfect comment or just the right question to ask that adds an extra twist to any research program. Working with him has been greatly stimulating and remarkably enriching.

Many thanks to Harold Ollivier and Wojciech Zurek, my two partners in crime, with who a part of this dissertation has been elaborated. The least I can say is this has been a very entertaining collaboration, through which I have learned enormously. I am also grateful to Charlie Bennett, Carl Caves, David Cory, Chris Fuchs, Camille Negrevergne, and Rob Spekkens for sharing their insights on some technical as well as conceptual aspects of this thesis.

I acknowledge the many other people with who I have had stimulating and enlightening discussions over the past three years on various scientific topics; in particular Howard Barnum, Jonathan Baugh, Alexandre Blais, Robin Blume-Kohout, Jean-Christian Boileau, Gilles Brassard, Fay Dowker, Artur Ekert, Joseph Emerson, Marie Ericsson, Ernesto Galvão, Florian Girelli, Daniel Gottesman, Patrick Hayden, Lucien Hardy, Dominik Janzing, Alexei Kitaev, Manny Knill, David Kribs, Frédéric Leblond, Etera Livine, Fotini Markopoulou, Gerard Milburn, Mike Mosca, Casey Myers, Juan Pablo Paz, Ruediger Schack, Lee Smolin, Rolando Somma, Raphael Sorkin, Alain Tapp, Hugo Touchette, Antony Valentini, Guifre Vidal, Lorenza Viola, Christof Zalka, Paolo Zanardi, as well as all the other members of the Institute for Quantum Computing and the Perimeter Institute.

I also acknowledge the Natural Sciences and Engineering Research Council of Canada, the Fonds Québécois de la Recherche sur la Nature et les Technologies, the The Canadian Institute for Advanced Research, the Canada Research Chairs, the Ontario Research and Development Challenge Fund, and Mike Lazaridis for financial support.

Je tiens a remercier chaleureusement tous mes amis et ma famille qui m’ont toujours supporté et encouragé, parfois malgré la distance. Vous comptez beaucoup pour moi et j’apprécie toujours énormément votre amitié. Enfin, un merci tout particulier à Isabelle pour tout le bonheur qu’elle m’apporte... et pour avoir dit oui.
À tous mes amis...
1 — Motivation

In my view the most fundamental statement of quantum mechanics is that the wavefunction, or, more generally the density matrix, represents our knowledge of the system we are trying to describe. [Pei91a]

—Sir Rudolph Peierls

Why is the world we perceive in our everyday life classical while the underlying laws of nature are quantum mechanical? The present dissertation is an attempt to provide answers to this question. Obviously, the only way we can hope to make any progress in addressing this old question is to first state it clearly, i.e. we must precisely describe what are the fundamental distinctions between a classical and a quantum behavior. This, on the other hand, often varies from one author to the other and is, we believe, responsible for the wide variety of interpretations of quantum theory — the distinct interpretations reflect the distinct perspective of the dissimilarities between the quantum and the classical.

We are thus forced to reveal ourselves on the outset: a clear statement of the question at the heart of this thesis forces us to choose an interpretation of quantum theory. Good! But before doing so, we would like to stress that the work presented in the next Chapters does not requires any commitment whatsoever to this interpretation. (In particular, it does not necessarily reflect the opinions of the collaborators of the present authors that were involved in projects related to this Thesis.) Interpretations of quantum theories are mostly concerned with explaining the strange worldview offered by quantum theory in terms of our classical preconceptions, for example by introducing non-local hidden variables. This Thesis instead starts with quantum theory and attempts to explain our “classical” everyday experience from it. Hence, the answers to the classicality problem put forward here — being operational in nature — are independent of any interpretation.
We simply believe that clarifying interpretational issues \textit{a priori} is the most efficient way of presenting and motivating the core problem addressed in this dissertation. Beside the main lines of thought followed in this dissertations, we note that our approach is also particularly well suited for the many-worlds interpretation, as well as consistent histories approaches to quantum mechanics.

\textit{The epistemic view}

We view the state $\rho(t)$ of a quantum system as a reflection of the \textit{subjective judgment of an observer} about this system. This \textit{epistemic} interpretation of quantum states, first clearly advocated by Einstein [How85a, Fin86a, EPR35a], inspired us mostly through the various writings of Carl Caves, Chris Fuchs, David Mermin, Asher Perez, and Rudiger Schack [CF96a, Per93a, FP00a, Mer01b, CFS02a, Fuc02c]. It is not our intention here to plead for an epistemic interpretation of quantum states: for this matter, we urge the reader to the above references, as well as to the admittedly incomplete yet compelling arguments put forward by Rob Spekkens [Spe04a].

In this sense, the classical analogue of a quantum state $\rho(t)$ is a probability density $P(x, p, t)$ over the phase space of a classical system. Indeed, for closed systems, they both follow Hamiltonian equations of motion: the quantum version known as Schrödinger’s equation $\dot{\rho} = -i[H, \rho]$ involves a commutator, and the classical version known as Liouville’s equation $\dot{P} = \{H, P\}$ involves a Poisson bracket. However, when measurements are performed on the systems and new information becomes available to the observer, \textit{the Hamiltonian evolution laws are no longer appropriate}. In the classical case, the update of the state given the newly acquired data $D$ is prescribed by Bayes’ rule

$$P(x, p) \xrightarrow{D} P(x, p|D) = \frac{P(D|x, p)P(x, p)}{P(D)} \tag{1.1}$$

where $P(D|x, p)$ is the probability of observing $D$ given that the system has phase space coordinates $(x, p)$, and $P(D)$ is the prior probability of $D$ given by

$$P(D) = \int P(D|x, p)P(x, p)dxdp. \tag{1.2}$$

In the quantum case, the state update rule given a projective measurement outcome $Q_j$ (the argument works just as well for POVMs) is

$$\rho \xrightarrow{Q_j} \rho_{|Q_j} = \frac{Q_j\rho Q_j}{P(Q_j)} \tag{1.3}$$
where the prior probability of the outcome $Q_j$ is prescribed by Born’s rule $P(Q_j) = Tr\{Q_j\rho\}$.

From this perspective, the “collapse of the wave function” per se has a classical analogue: the state assigned to a system by an observer may change abruptly when new data are made available to him. Thus, the state disturbance caused by a measurement is not a purely quantum phenomenon: measurements carried on classical systems can disturb their states just as well. Viewing quantum states as analogue of classical probability distributions is a good way of getting rid of a large amount of the spooky-ness in quantum theory, such as the apparent “action at a distance” known as remote steering [How85a, Fin86a], the no cloning theorem [WZ82a, Die82b, DPP02a], the impossibility of perfectly distinguishing non orthogonal states [Che00a, RS03a], etc. (see also [Spe04a]).

**Distinction between quantum and classical**

What is unique to the classical case however is a peculiarity that follows from Bayes’ update rule:

$$\sum_D P(x, p|D)P(D) = P(x, p). \quad (1.4)$$

In words, averaging the post-measurement state $P(x, p|D)$ over all possible measurement outcomes $D$ is like not carrying any measurement at all, or in other words, carrying a measurement without looking at its outcome is like not doing anything. This is generally not true for measurements carried on quantum systems

$$\sum_j \rho_{Q_j} P(Q_j) = \sum_j Q_j \rho Q_j \neq \rho, \quad (1.5)$$

unless very special conditions are met.

The consequence of this special feature of Bayes’ update rule is that there exist in the classical theory states of complete knowledge that are not affected by any measurements. Indeed, when the density over the classical phase space is a delta function $P(x, p) = \delta(x - x_0)\delta(p - p_0)$, the prior probability of the data $D$ given by Eq. (1.2) will be $P(Y) = P(Y|x_0, p_0)$, so the state update rule Eq. (1.1) yields

$$P(x, p|D) = \frac{P(D|x, p)\delta(x - x_0)\delta(p - p_0)}{P(D|x_0, p_0)} = P(x, p); \quad (1.6)$$
there is no “collapse of the probability density”, regardless of the measured quantity. This urges us to adopt the following interpretation for these states of complete knowledge: they are objective elements of physical reality. Indeed, due to the above observation, we can safely say that classical systems always occupy a certain position \( x_0 \) and have a certain momentum \( p_0 \) that can be discovered — without being disturbed — through measurements. The classical states \( P(x, p) \) reflects our (possibly incomplete) knowledge about these objective properties of the system. Hence, the information in \( P(x, p) \) is information about the actual phase space coordinates of the system. This is also reflected by Eq. 1.2: we assign a probability \( P(D|x, p) \) to the data \( D \) as if the system had objective phase space coordinates \( (x, p) \), and then average over all possible coordinates to obtain the prior distribution \( P(D) \) for the value of \( D \).\(^1\)

Although quantum states and classical probability distributions have a lot of properties in common, there is no quantum analogue to these classical states of complete knowledge.\(^2\) In particular — and as opposed to quantum states and classical states of incomplete knowledge — classical states of complete knowledge cannot exhibit any correlations, they can be cloned, they can always be perfectly distinguished, and as just demonstrated, they are not disturbed by any measurements. The lack of a quantum analogue of these classical states of complete knowledge is, we argue, the main distinction between the quantum and the classical world. Classical states encapsulate our knowledge about the objective properties of the system, i.e. about its phase space coordinates that are associated to states of complete knowledge. Meanwhile, quantum states are also viewed as states of knowledge, but it is not clear what this knowledge is about. Moreover, Bell’s theorem [Bel64a] and Kochen-Specker theorem [KS67a] tell us that the information in a quantum state cannot be about local and noncontextual hidden variables. This is in fact the main criticism to the epistemic interpretation of quantum states.

\(^{1}\)The above definition of “states of complete knowledge” does not imply that under such a state assignment the outcome of any measurement is deterministic. For example, one can imagine a finite accuracy measurement of the position of a classical particle with overlapping outcomes (e.g. described in terms of some overlapping Gaussian distributions). The outcome of such measurements is not deterministic even when \( P(x, p) = \delta(x - x_0)\delta(p - p_0) \). However, there is no state disturbance.

\(^{2}\)In a certain sense, pure quantum states can be called “states of maximal knowledge” which differs from our notion of “complete” knowledge, i.e. that they are not disturbed by any measurement.
Two questions

We find ourselves in an awkward situation: if quantum theory is the correct theory of nature, then it should encapsulate classical theory as a special case. But classical theory admits objective elements of reality, while it is not clear how they fit in the quantum theory (although they would be greatly appreciated to establish a connexion with the physical reality). This raises two important questions:

Q1 How can the objective properties of classical systems emerge from the underlying quantum theory?

Q2 What is the information in a quantum state about?

If one is willing to accept an arbitrary “split” between the quantum and the classical world — such as prescribed by Bohr [Boh28a] and the Copenhagen interpretation — a simple answer to the second question Q2 is that this knowledge is about the outcomes of future measurements. This is the line of thoughts followed by Fuchs [Fuc02c] for example. However, as will be argued in Section 2.2, even if we accept the outcomes of measurements as classical “by decree”, we still need to explain how a consensus about the properties of a system can be reached by several observers acquiring their information through independent measurements — a prerequisite for the emergence of objectivity. Indeed, unless the various observers pre-agree on what is to be measured on the system, their independent measurement will typically reveal inconsistent information about the system; more on this in the next Chapter.

In any case, our starting point here is that quantum mechanics is basically the correct theory of nature, and everything — including measurement apparatus — is governed by its laws. Our goal is thus to provide a mechanism within this theory that explains the emergence of the classical objective reality (as described above) we experience.

---

3Of course, Chris would disagree with this description of his program! Through our correspondence with him, we have come to understand that it is possible to think of quantum theory as a good way of reasoning “about reality”, at the price of revisiting the very notion of reality. In a nutshell, our understanding of his point of view is that reality is being formed by our intervention into the world, i.e. by our measurements. From this perspective, not only do quantum measurements provide us information about the physical reality, but it “provokes” its existence. Although we sympathize with this point of view, it is slippery territory that we do not want to venture here. Rather, throughout this dissertation, we stick to the narrow-minded concept of reality described above, and leave the philosophical debates about the meaning of reality to philosophers.
Most interpretations of quantum theory are attempts to explain the worldview offered by quantum theory in terms of our classical preconception, for example by introducing hidden variables. This Thesis follows a different path: we assume that quantum theory is correct and show how it leads to the classical world we perceive and which gives rise to our classical preconception. Our explanations of the classical are valid as long as the quantum formalism is unchanged, and are therefore independent of any interpretation. In particular, as mentioned in the opening paragraph, our approach is also particularly well suited for many-world interpretation and consistent histories.

Our proposal

We will provide an answer to the first of the two questions Q1 & Q2 by a careful analysis of the special circumstances in which we acquire information about the “classical world”. The two mechanisms we identify are

- The indirect measurement of the properties of the system of interest through the redundant proliferation of information in its environment.
- The direct measurement of “macroscopic” properties of the system of interest.

These two mechanisms will be the object of study of Chapters 2 and 3 respectively. We strongly believe that all the information that is made available to our senses falls under one of these two categories\(^4\). Independent observers whose information gathering capacities are limited to those two mechanisms will unavoidably arrive at a consensus about the properties of the world: they will reach an inter-subjective agreement. Of course, the fact that several independent observers all agree on something does not imply that this thing really exists. However, we believe that this is as close as one can get to objectivity without modifying quantum theory, e.g. by adding an objective collapse mechanism [GRW86a]. Moreover, physics cannot distinguish such an operational notion

\(^4\)Note that this can be in an induced fashion, like through the chain of interaction: quantum system - measurement apparatus - output display - photon environment - retina. This “von Neumann chain” would induce objective properties to the original quantum system since information about it becomes redundantly imprinted in the environment. Moreover, it will often be a combination of both mechanisms that will provide us with our information, e.g. a macroscopic number of photons can hit our retina, providing us visual data.
of objectivity from true objectivity: as far as we can tell, the objective classical states we
encounter in our everyday life might also just reflect an inter-subjective agreement.

This part of the program will be formally carried through à la Copenhagen by granting
a special role to measurement processes. However, and this is absolutely crucial,
measurements are not a building block of our program. Rather, we use hypothetical
measurements as a way to characterize the correlations among different physical sys-
tems. In the words of Wheeler: “The theory of observation becomes a special case of
the theory of the correlations between subsystems” [Whe57a]. This is of course in the
spirit of Everett’s original “relative state” interpretation of quantum theory [Eve57a],
but differs from the “many-world” interpretation that has emerged from it since quan-
tum states are viewed as subjective here. Rovelli’s formulation of the relative state
interpretation [Rov97a] is perhaps closer to the interpretation which will emerge from
the present Thesis: quantum theory prescribes what are the possible relations between
different systems. The variety of possible correlations between quantum systems is much
wider than that allowed by classical theory — as illustrated by the violation Bell’s in-
equalities [Bel64a, AGR81a] — yet, these correlations are not arbitrary (for example,
“entanglement is monogamous” [TWD03a]). It is by carefully analyzing the limitations
imposed on these correlations by quantum theory, combined with the limited informa-
tion gathering capacities of observers, that we will demonstrate how a consensus
between independent observers about the outcome of hypothetical measurements can
emerge from within quantum theory.

In this relational approach [Rov97a], there is a priori no distinction between systems
and observers: an observer can assign a quantum state to any other system, including
other observers. However, when one of the correlated systems turns out to be an ob-
server, his correlation to other systems are, from his own perspective, information about
these other systems. Correlations — and in particular those between an observer and a
system of interest — are what gives rise to our perception of the world, and hypothetical
measurements are a good way to characterize these relations.

This leaves open the second question Q2. Having established that quantum states
represent observers’ knowledge, and that under certain circumstances independent ob-
servers will agree on their state assignment, it remains to be clarified what exactly this
knowledge is about. This is the million dollar question of the epistemic interpretation,
and to our taste, remains an open one. The above discussion suggests the following
speculative answer: quantum states represent information about those things on which we can potentially all agree.

This answer is similar to Fuchs’, but has an extra twist. Instead of admitting an arbitrary split between the quantum and the classical, we recognize that there is room in quantum theory — given realistic assumptions about how we gather our information — for inter-subjective agreement about certain properties of the world. These singled-out properties — which include measurement outcomes — are therefore the only object of interest to physical theories, as they can be discovered by independent observers, who can later compare their findings. Information in quantum states is thus about these preferred properties of the world that behave as “classical”. Thus, we came a long way to finally agree that this information is about the outcome of future measurements. We simply took a huge detour to justify our point of view, i.e. to show that it does not require any modification to quantum theory.

1.1. Outline of the dissertation

The main purpose of this thesis is to provide answers to the first question Q1 proposed above: How can the objective properties of classical systems emerge from the underlying quantum theory? For this, we will study the two main mechanisms we have identified, and show how they lead to an operational notion of objectivity. Chapter 2 will focus on the information that can be learned about the system by an observer limited to perform measurements on small fragments of the system’s environment. An example of this mechanism is the photon environment responsible for all our visual data. The only information about the system that can be learned in this fashion is about its properties that are redundantly imprinted in its environment. We will show that redundant proliferation of information in the environment implies the selection of a preferred system observable. Many independent observers monitoring the environment will thus learn about this observable — and only about this observable — leading to the emergence of a consensus among them.

In Chapter 3, we study the effect of measurement of collective properties on macroscopic ensemble of quantum systems. Our tactile information is a good illustration of this mechanism: when the tip of our finger touches an object, it interacts collectively with a very large number of molecules. In particular, we will demonstrate a trade-off between the disturbance caused to the state of an ensemble of identically prepared
quantum systems and the measurement coarseness, as a function of the size of the ensemble. As we will show, given that there is no entanglement on macroscopic scale in the ensemble, these measurements will behave as if they were revealing an underlying objective element of reality, namely the average reduced state of a single system. For an observer limited to the measurement of such macroscopic quantities, the ensemble behaves just like a classical system and Bayes' update rule can be consistently applied.

While the second question Q2 — as to know what is the information in a quantum state about — is not the main focus of this dissertation, we will often comment on it since we believe that our work strongly hints upon it. We do not claim to have provided a definite answer to it — nor do we believe anyone else has — but simply wish to explore the new and promising avenue provided by our answer to the first question Q1. As a consequence, we may end up with more questions than answers, which in any case are speculative. Finally, the interpretation outlined in this introduction as well as the main achievement of this dissertation will be summed up in the last Chapter 4.

1.2. Additional information for the examiners of this thesis

This dissertation is mainly composed of three articles. Chapter 2 presents the ideas studied in an article [OPZ03a] written with Harold Ollivier and Wojciech Zurek entitled “Objective properties from subjective quantum states: Environment as a witness” available on the physics archive as quant-ph/0307229, and published in Physical Review Letters 93 220401. The chapter is essentially a version of a second longer research article [OPZ04a] written with the same co-authors entitled “Environment as a Witness: Selective Proliferation of Information and Emergence of Objectivity”, also available on the physics archive as quant-ph/0408125, and submitted to Physical Review A.

The contribution of the present author to these articles is the following. The idea of using redundancy as a way to characterize the classicality of certain physical observables was first suggested in an early version of Zurek’s review paper on decoherence, quant-ph/0105127v1. The work presented here is a refinement of this rough idea that was realized through several animated discussions between all three authors that took place over a three year period. These discussions have also influenced Zurek’s vision of the role of redundancy in the quantum-classical transition as is reflected by the final version of his review on decoherence [Zur03a]. In particular, we have introduced information-theoretic tools to measure redundancy, which has enable us to derive several formal
results. The questions of prime importance were raised during these discussions. Most of the mathematical work (proof of theorems, numerical calculations) was then carried out by Ollivier and the present author. Finally, the first drafts of the manuscripts were written by Ollivier and the present author, and then went through a long and fruitful “remodeling” process in which all three authors were involved, once again giving rise to animated and stimulating discussions and email exchanges!

Chapter 3 is essentially a version of an article [Pou04a] written by the present author entitled “Macroscopic observables” available on the physics archive as quant-ph/0403212, and accepted for publication in Physical Review A. The main motivation for this research was to characterize the fundamental disturbance caused by measurements carried on ensemble of quantum systems, such as those used in liquid state nuclear magnetic resonance.

These three articles were written for purposes slightly different than the motivation given in this introduction, which reflects the present author’s personal interpretation. As a consequence, we have decided to keep the original introductions of the articles as parts of the following chapters. These introductions will place the specific problems addressed in each chapters in a more general context than the narrow point of view expressed so far (which, we repeat, is not necessarily shared by Ollivier and Zurek). This is done at the cost of a small amount of redundancy, which is a good thing! (This is actually a bad joke which should get clarified in the next Chapter.) Moreover, we have added several comments throughout the original articles to keep a clear relation with the problems of central interest of this Thesis, and to emphasize the personal interpretation of the present author.

Finally, all other articles published by the present author during his Ph.D. program have been attached in Appendix C of the dissertation. These articles are not directly related to the main Thesis developed here; they have only been included for completeness.
Summary of Chapter 1

- The state $\rho$ of a quantum system, just like a probability density $P(x, p, t)$ over the phase space of a classical system, is not an objective element of reality: it reflects the subjective knowledge of an observer about this system.

- There exists classical states of complete knowledge that are — at least in an operational sense — objective elements of reality: they can be discovered by independent observers without getting disrupted in the process. Hence, the knowledge encapsulated in a probability density $P(x, p, t)$ is about these objective states.

- This leaves two questions open:
  1. How can the objective properties of classical systems emerge from the underlying quantum theory?
  2. What is the information in a quantum state about?

- Our proposed answer to question 1.: Through the restrictions imposed on correlations between various systems by quantum theory together with the limited information acquisition capacities of the observers. These limitations are:
  1. The indirect measurement of the properties of the system of interest through the redundant proliferation of information in its environment.
  2. The direct measurement of “macroscopic” properties of the system of interest.

- Our proposed answer to question 2.: It is about those properties of the world that can be discovered and compared by different observers, and which should be the only objects of interest to physical theories. These objective properties are singled out by the two mechanisms outlined above.
But then I fell into bad company. I started hanging out with the quantum computation crowd, for many of whom quantum mechanics is self-evidently and unproblematically all about information. [Mer01a]

—N. David Mermin

2.1. Introduction

Emergence of a classical reality from the quantum substrate has been the focus of discussions on the interpretation of quantum theory ever since its inception. This problem has been extensively studied, primarily in the context of quantum measurements. Bohr’s solution proposed in 1928 [Boh28a] introduced the classical domain “by hand”, with a demand that much of the universe — including measuring apparatuses — must be classical. This Copenhagen interpretation proved to be workable and durable, but is ultimately unsatisfying, because of the arbitrary split between quantum and classical domains of the Universe. Thus, Copenhagen interpretation notwithstanding, attempts to explain the emergence of the classical, objective reality (including measurement outcomes) using only quantum theory were made ever since its structure became clear in the late 1920’s (see e.g. [WZ83a] and references therein).

Von Neumann [vN55a] has introduced a particularly influential model of the measurement process. In this approach, the apparatus $\mathcal{A}$ is quantum. The generic example consists of a 2-dimensional system $\mathcal{S}$ in pure state $\alpha|0\rangle + \beta|1\rangle$ that gets “measured” by a 2-dimensional apparatus initially in state $|\mu\rangle_A$. In course of the measurement the apparatus becomes — as one would say using modern language — entangled with the system $\mathcal{S}$:

$$ (\alpha|0\rangle + \beta|1\rangle) \otimes |\mu_A\rangle \rightarrow \alpha|0\rangle \otimes |\mu^A_0\rangle + \beta|1\rangle \otimes |\mu^A_1\rangle. $$ (2.1)

This entanglement, known as pre-measurement, implies correlation of $\mathcal{S}$ and $\mathcal{A}$. This suggests a relative state interpretation of quantum theory [Eve57a, Zeh73a], and raises
the issue of the basis ambiguity [Zeh73a, Zur81a]: different observables of $A$ are correlated with incompatible sets of pure states of the system. For example, the states $\{|\mu_0^A\rangle, |\mu_1^A\rangle\}$ of $A$ are in one-to-one correlation with the states $\{|0\rangle, |1\rangle\}$ of $S$, while the states $\{(|\mu_0^A\rangle \pm |\mu_1^A\rangle)/\sqrt{2}\}$ are in one-to-one correlation with the states $\{(\alpha|0\rangle \pm \beta|1\rangle)/\sqrt{2}\}$ of $S$. Thus, von Neumann’s model does not explain the existence of a fixed “menu” of possible measurement outcomes — an issue that must be addressed before the apparent selection of one position on this menu (i.e. the “collapse of the wave-packet”) is contemplated.

Decoherence theory [Zur91a, GJK+96a, PZ01a, Zur03a] added a new element to von Neumann’s measurement model: in addition to $S$ and $A$, decoherence recognizes the role of the environment $E$ that surrounds $A$ and interacts with it (or whatever object is immersed in it). The resulting “openness” of $A$ invalidates the egalitarian principle of superposition: while all states in the Hilbert space of the apparatus $A$ are “legal” quantum superpositions, only some of them will be stable. Returning to our example, the environment may interact with $A$ in such a way that an arbitrary superposition $\xi_0|\mu_0^A\rangle + \xi_1|\mu_1^A\rangle$ is transformed into a mixture $|\xi_0|^2|\mu_0^A\rangle\langle\mu_0^A| + |\xi_1|^2|\mu_1^A\rangle\langle\mu_1^A|$ after a very short time. Thus, only the two states $|\mu_0^A\rangle$ and $|\mu_1^A\rangle$ remain pure over time. Selection of such preferred set of states is known as environment-induced superselection, or einselection. The persistence of the correlation between $A$ and $S$ is the desired prerequisite of measurement, and only the stable pointer basis of $A$ selected by the interaction with $E$ fits the bill [Zur81a, Zur82a, PZ01a, Zur03a]. Indeed, after the decoherence time, the joint state of $S$ and $A$ Eq. (2.1) becomes the mixed state

$$|\alpha|^2|0\rangle\langle0| \otimes |\mu_0^A\rangle\langle\mu_0^A| + |\beta|^2|1\rangle\langle1| \otimes |\mu_1^A\rangle\langle\mu_1^A|.$$  

(2.2)

As a consequence, only the correlations of $A$ with the system states $\{|0\rangle, |1\rangle\}$ persist.

In its conventional formulation, decoherence theory treats the information transferred to $E$ during its interaction with $S$ as inaccessible. However, in the real world, this is typically not the case. Indeed, we gain most of our information by intercepting a small fraction of the environment — mostly photons and phonons — and this is significant for the emergence of effectively classical states from the quantum substrate [Zur93b, Zur98a, Zur00a]. The purpose of this Chapter is to investigate the consequences of such an indirect information acquisition for the quantum-classical transition. Quantum Darwinism (the dynamics responsible for the proliferation of correlations that
leads to the *survival of the fittest information* is a natural complement to this *environment as a witness* point of view, focused on the data about $S$ that can be extracted by interrogating $E$. This is a dramatic twist in the story that goes well beyond the decoherence approach. As we shall demonstrate, the manner in which the information is stored in the environment is the reason for the consensus among many observers about the state of effectively classical (but ultimately quantum) systems. In other words, the structure of information deposition in $E$ is responsible for the emergence of the objective classical reality from the quantum substrate.

In the next section, we motivate the need for a study of classicality focused on the information about the system $S$ stored in the environment. This will be driven by the fact that objective properties of quantum systems (to be operationally defined in Section 2.2) cannot in general be “found out” through direct measurements. Sections 2.3 and 2.4 set up the notation and introduce tools of information theory required for the present study. Section 2.5 contains the core information-theoretic analysis of the Chapter. There, we establish a number of facts about the structure of the information stored in the environment, and draw consequences for system observables that are redundantly imprinted in $E$. These general properties are then illustrated in Section 2.6 on a dynamical model used extensively in the study of decoherence. This allows us to extend the results of our analysis, and establish a direct connection between einselection and the emergence of an objective classical reality. Finally, we consider some open questions in Section 2.7 and conclude in Section 2.8 with a summary of Quantum Darwinism.

### 2.2. Objectivity: what is the problem?

The pointer states of $S$ singled out by einselection are robust in the sense that they, or their dynamically evolved descendants, continue to faithfully describe the system in spite of the interaction with $E$. This property — predictability — is shared by the states of classical systems, and is thus taken as a sign of the emergence of a classical reality. Moreover, einselection generally tends to banish flagrantly quantum superpositions, but retains classical-looking states that are localized.

The loss of validity of the egalitarian principle of superposition is a significant step forward in the understanding of the quantum-classical transition, but it does not go all the way: the einselected pointer states are still ultimately quantum and, thus, remain sensitive to direct measurements — a purely quantum problem. An observer trying to
find out about the system directly will generally disturb its state, unless he happens
to make a non-demolition measurement \[CTD+80a, BK96a\] in the pointer basis. As a
consequence, it is effectively impossible for an initially ignorant observer to learn about
the system through a direct measurement without perturbing it. After a measurement,
the state of the system will be what the observer finds out it is, but not — in general
— what it was before. This is a manifestation of the absence of “states of complete
knowledge” in quantum theory that describe an underlying objective reality.

The situation becomes even more worrisome when one considers many initially ig-
norant observers attempting to find out about the system. As a consequence of the
unavoidable disturbance caused by a direct measurement on the system, the informa-
tion gained by the first observer’s measurement gets invalidated by the second observer’s
measurement, etc., unless they all happen to measure in the same basis — or more pre-
cisely, unless the measured observables share the system’s pointer states as eigenstates.
Therefore, it is impossible for many observers to arrive at a consensus about properties
of the system without a prior agreement of what is to be measured: a consensus cannot
emerge when the measurements are direct, it can only be imposed a priori! This is a dra-
matic departure from classical physics, where many ignorant observers can — at least
in principle — find out the state of the system without modifying it. In short, classi-
cal systems admit an underlying objective description, a “classical reality” described in
terms of phase space coordinates, that can be found out by initially ignorant observers.
This is generally not the case for quantum systems.

Quantum Darwinism \[Zur03a, OPZ03a\] aims to demonstrate that a consensus about
the properties of a quantum system — the key symptom of classical reality — arises
from within quantum theory when one recognizes the role of the environment as a
broadcasting medium that acquires multiple copies of the information about preferred
properties of the system of interest.

We will set up an operational framework for the analysis of the emergence of objective
classical reality of quantum systems. This requires a precise operational definition
of objectivity. We adopt the following one (these requirements are not meant to be
independent of each other):

**Definition 2.2.1 (Objective property).** A property of a physical system is objective
when it is

1. simultaneously accessible to many observers,
2.2. Objectivity: what is the problem?

2. who are able to find out what it is without prior knowledge about the system of interest, and

3. who can arrive at a consensus about it without prior agreement.

This operational definition of what is objective is inspired by the notion of “element of physical reality” used by Einstein, Podolsky and Rosen in their famous paper [EPR35a] on entanglement:

If, without in any way disturbing a system, we can predict with certainty (i.e. with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity. [...] Regarded not as a necessary, but merely as a sufficient condition of reality, this criterion is in agreement with classical as well as quantum-mechanical ideas of reality.

Any property of the system fulfilling this requirement would be considered an element of objective reality according to the definition we adopt.

In our definition, we have not insisted on the notion of determinism like EPR have. However, the key feature of objectivity, the emergence of a consensus among several observers, is intimately related to determinism. Independent observers are able to predict the outcome of some measurements on the system. It is not the fundamentally indeterministic nature of quantum theory that clashes with our conception of the classical, but the lack of an objective reality. However, like Einstein, we find it hard to separate the two notions: (quote of Pauli taken from [Mer85a])

In particular, Einstein does not consider the concept of ‘determinism’ to be as fundamental as it is frequently held to be [...]. In the same way, he disputed that he uses as criterion for the admissibility of a theory the question: ‘Is it rigorously deterministic?’.

As it follows from the discussion above, our definition (as well as the one of EPR) rules out arbitrary direct measurements as means to acquire objective information about a quantum system. Thus, objective information about quantum systems must be acquired either by a constrained set of pre-agreed direct measurements on $\mathcal{S}$, or indirectly — i.e., using the environment as a communication channel. The former scenario will be studied in the next Chapter (see also [Gra02a]); for now, we focus on the information
about $S$ that can be learned through $E$. In absence of any structure of $E$, this is still insufficient to explain the emergence of a consensus about the properties of $S$. Measurements on the environment suffer from the same problems as direct measurements on the system: they can be performed in arbitrary bases and generally disturb the state of the environment, and hence, the correlations between $S$ and $E$. For instance, when an observer performs a measurement on the environment, he might “spoil” the correlation with the system. Unless all observers had agreed to measure the environment in the same basis, their subsequent measurements on the environment might not yield the desired information about the system.

The solution to this problem becomes obvious after a closer inspection of what happens in the real world: not only is information about the system acquired indirectly by probing the environment, but different observers acquire their data by probing different fragments of $E$. By definition, when the same information about $S$ can be discovered from different fragments, it must have been imprinted in the environment redundantly: each fragment of $E$ must contain a relatively good copy of it. In addition, when many disjoint fragments of the environment contain information about some properties of the system, they can be accessed by different observers without the danger of invalidating each other’s conclusions. This is because observables acting on disjoint fragments of $E$ always commute with each other. Therefore, ignorant observers can vary their measurements independently, corroborate their own results and arrive at a description of the properties of the system. Hence, the first two requirements for objectivity are satisfied.

Moreover, and this is a crucial result of our study, we will demonstrate that redundant imprinting in the environment can only be achieved for a unique system observable. In other words, the environment-promoted amplification of information required to arrive at a redundant imprinting comes at the price of singling out a unique system observable. As a consequence, even initially ignorant observers performing arbitrary measurements on their fragment of $E$ will find out about this unique observable. This establishes that redundant imprinting in the environment is a sufficient requirement for the emergence of classical objective reality. We shall thus identify the existence of an objective property of the system with the existence of its complete and redundant imprint in the environment.

Quantum Darwinism makes novel use of information theory by focusing on the communication capacity of the environment. This is a departure from conventional
“system-based” treatments of decoherence. There, the environment is only an “information sink”, a source of decoherence responsible for irreversible loss of information [Zur81a, ZHP93a, GJK+96a, PZ01a]. However, these two complementary approaches do agree on their conclusions: as we will show, the pointer observable singled out by einseletion is the only one that can leave a redundant imprint on the environment. This can be understood as a consequence of the ability of the pointer states to persist while immersed in the environment. Moreover, in both approaches predictability of the preferred states of the system (i.e., either from initial conditions, or from many independent observations on $\mathcal{E}$) is the key criterion. This predictability is tied to the resilience that allows the information about the pointer observables to proliferate, very much in the spirit of the Darwinian “survival of the fittest”.

2.3. Definitions and conventions

In the setting we are considering, a system $S$ with Hilbert space $\mathcal{H}^S$ interacts with an environment $\mathcal{E}$ with Hilbert space $\mathcal{H}^\mathcal{E}$. We denote the dimension of these state spaces by $d^S$ and $d^\mathcal{E}$ respectively. Furthermore, we assume that the environment is composed of $N$ environmental subsystems $\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_N$. That is, its Hilbert space has a natural tensor product structure $\mathcal{H}^\mathcal{E} = \bigotimes_{k=1}^{N} \mathcal{H}^{\mathcal{E}_k}$. This partition plays an important role in our analysis, as it suggests a natural definition of the independently accessible fragments of $\mathcal{E}$. We will comment on it at the end of Section 2.4.

The joint quantum state of $S$ and $\mathcal{E}$ is described by the density operator $\rho^{SE}$ defined on $\mathcal{H}^S \otimes \mathcal{H}^\mathcal{E}$. The reduced state of the system is obtained by “tracing out” the environment $\rho^S = \text{Tr}_\mathcal{E}\{\rho^{SE}\}$. It will often be useful to consider the joint state of the system and a fragment of the environment. Such fragment — i.e. a subset of $\mathcal{E} = \{\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_N\}$ — will be denoted by $\mathcal{F}$. The reduced state of $S$ and $\mathcal{F}$ is obtained by tracing out the complement of $\mathcal{F}$: $\rho^{SF} = \text{Tr}_\overline{\mathcal{F}}\{\rho^{SE}\}$, where $\overline{\mathcal{F}} = \mathcal{E} - \mathcal{F}$.

Following textbook quantum mechanics, we call “observable of $S$” (resp. of $\mathcal{E}$) any Hermitian operator acting on $\mathcal{H}^S$ (resp. $\mathcal{H}^\mathcal{E}$). In this Chapter, we will use the first letters of the alphabet $A, B, C$ to denote system observables while the last letters $X, Y, Z$ will be reserved for environment observables. Hermitian operators can be written in their spectral decomposition:

$$A = \sum_j a_j A_j.$$ (2.3)
Adding to our convention, observables are denoted by bold capital letters, their eigenvalues by lowercase letters, and spectral projectors by capital letters. Only the spectral projectors are of interest to us as they completely characterize the measurement process, and the correlations between observables.

In the present Chapter, the words “system” and “environment” are used in a very broad sense. Without loss of generality, we will suppose that $\mathcal{H}^{S}$ is that part of the Hilbert space of $S$ that contains the degrees of freedom of interest. Even when the system is macroscopic, e.g. a baseball, we are typically only interested in a few of its degrees of freedom, e.g. center of mass, local densities, etc. Moreover, the degrees of freedom of $S$ that do not couple to $E$ play no role in our analysis. Hence $d^{S}$ can remain reasonably small even for fairly large systems: $d^{S}$ is really the number of relevant distinct physical configurations of $S$. This considerably simplifies the notation without compromising the rigor of our analysis.

Similarly, it is not necessary to incorporate “all the rest of the Universe” in $E$. The number $N$ really counts the number of environmental subsystems that may have been influenced by the system: only they may contain information about $S$. Hence, in many situations of interest — like a photon environment scattering off an object — the “size” of relevant $E$ can grow over time.

2.4. Information

The approach to classicality outlined above is based on the existence of correlations between $S$ and its environment that can be exploited by various observers to find out about the system. As both $S$ and $E$ are quantum systems, quantum information theory may appear to be the appropriate tool to study these correlations. This avenue has been proposed in the past [Zur00a, Zur03a] in parallel with the approach we pursue here and is currently also under investigation [BKZ04a]. However, the emphasis here is on the physical properties of the system, and information about them is easier to characterize through the relevant hypothetical measurements. We focus on what can actually be found out about various observables of the system by monitoring observables in fragments of the environment. For these reasons, we base our investigation on classical information theory [CT91a].

Accordingly, the core question we ask is: how much does one learn about observable $A$ by measuring a different observable $X$? This question has an operational meaning.
An observer may be considering measurement of the observable $A$, but cannot predict its outcome with certainty. To reduce his ignorance, he can choose to measure a different observable $X$. By doing so, he may decrease his uncertainty about the value of $A$. The amount by which his uncertainty decreases is precisely the information gain we are going to study. It represents the average number of bits required to write down, in the most efficient way, the relevant data about $A$ acquired through the measurement of $X$.

We will mostly be interested in the case where $A$ acts on the system and $X$ acts on a fragment of the environment — which automatically implies that $[A, X] = 0$. However, we will occasionally need to consider the correlations between the measurements carried successively on the same system: hence, we present here the general case and return to the special case of commuting observables in the next section. Thus, $A$ and $X$, with spectral projectors $A_i$ and $X_j$, are arbitrary physical observables acting on an arbitrary system, in state $\rho$. (There is no environment here, just one system and two observables that may or may not commute.)

The observer’s uncertainty about the measurement outcome of $A$ is given by the corresponding Shannon entropy:

$$H(A) = - \sum_i P(A_i) \ln P(A_i)$$  \hspace{1cm} (2.4)

where the probability associated with the measurement outcome “$i$” — with the spectral projector $A_i$ — is given by Born’s rule $P(A_i) = \text{Tr}\{A_i\rho\}$. Entropy measures ignorance about the value of $A$, the average number of bits missing to completely determine its value. When the measurement of observable $X$ is performed and outcome $X_j$ is obtained, the state of the system is updated to

$$\rho \xrightarrow{X_j} \rho_{X_j} = \frac{X_j\rho X_j}{P(X_j)}$$  \hspace{1cm} (2.5)

according to the projection postulate of quantum theory [vN55a]. This state update changes the probability assignment of the measurement outcomes of $A$:

$$P(A_i|X_j) = \text{Tr}\{A_i\rho_{X_j}\} = \frac{\text{Tr}\{A_iX_j\rho X_j\}}{P(X_j)}.$$  \hspace{1cm} (2.6)

It is customary to call $P(A_i|X_j)$ “the conditional probability of $A_i$ given $X_j$” and similarly, $\rho_{X_j}$ is “the conditional state of the system given $X_j$.”
Thus, when $A$ is measured subsequently to $X$, the randomness of its outcome would be characterized by:

$$H(A|X_j) = -\sum_i P(A_i|X_j) \ln P(A_i|X_j).$$

The conditional entropy of $A$ given $X$ is the average of this quantity over the measurement outcomes of $X$: $H(A|X) = \sum_j P(X_j)H(A|X_j)$. The difference between the initial entropy of $A$ and its entropy posterior to the measurement of $X$ defines the mutual information

$$I(A : X) = H(A) - H(A|X).$$

This is the average amount of information about $A$ obtained by measuring $X$.

In quantum mechanics, it is possible that a certain measurement decreases one’s ability to predict the outcome of a subsequent measurement, so mutual information is not necessarily positive. This is in fact the reason why direct measurement on the system cannot be used to arrive at a consensus about the state of the system. Measurement by one observer will invalidate the knowledge acquired by another when their measurements do not commute. However, this disturbance can be avoided when the measurements are carried out on different subsystems, as then the observables commute automatically. The mutual information between such observables has extra properties that we shall now describe.

**Correlations between system and environment**

Let us now consider the case where $A$ acts on $S$ and $X$ on $E$, or on a fragment $F$ of $E$. As $[A, X] = 0$, the order in that the measurements are carried out does not change joint probability distribution $P(A_i, X_j) = \text{Tr}\{A_iX_j\rho\} = \text{Tr}\{X_jA_i\rho\}$. It follows from Eqs. (2.5-2.8) that the mutual information defined above can be written in an explicitly symmetric form:

$$I(A : X) = \sum_{ij} P(A_i, X_j) \ln \frac{P(A_i, X_j)}{P(A_i)P(X_j)}$$

$$= H(A) + H(X) - H(A, X).$$

The amount of information about $A$ that is obtained by measuring $X$ is equal to the amount of information gained about $X$ by measuring $A$, and is always positive. In this
2.4. Information

Figure 2.1: Venn diagram for classical information. $H(A)$ is the entropy associated with a measurement of $A$: it is the information needed to completely determine its outcome. $H(X)$ is the same quantity for the observable $X$. $H(A, X)$ is the joint entropy of $A$ and $X$. $H(A|X)$ is the average uncertainty about $A$ remaining after a measurement of $X$. The information learned about $A$ by measuring $X$ is thus $I(A : X) = H(A) - H(A|X)$. The equivalent definition $I(A : X) = H(A) + H(X) - H(A, X)$ can also be understood from the diagram. These two definitions of the mutual information are equivalent [CT91a] when probabilities can be consistently assigned to the outcomes of all the possible measurements of $A$ and $X$ both separately and jointly: this is ensured when $A$ and $X$ commute. They need not coincide otherwise.

In particular, the maximum amount of information about the system observable $A$ that can be retrieved from the entire environment is denoted by $\hat{I}_E(A)$. This quantity plays a crucial role in our analysis as only when $\hat{I}_E(A) \approx H(A)$ can we hope to “find out” about $A$ by probing the environment: the amount of information in the environment, $\hat{I}_E(A)$, must be sufficiently large to compensate for the observer’s initial ignorance, $H(A)$, about the value of $A$. 
**Redundancy of information in the environment**

When \( \hat{I}_E(A) \approx H(A) \), the value of \( A \) can be found out indirectly by probing the environment. However, as argued in Section 2.2, for many observers to arrive at a consensus about the value of an observable \( A \), there must be many copies of this information in \( \mathcal{E} \). As a consequence, independent observers will be able to perform measurements on disjoint subsets of the environment, without the risk of invalidating each other’s observations.

*Redundancy* is therefore defined as the number of disjoint subsets of the environment containing almost all — all but a fraction \( \delta \) — of the information about \( A \) present in the entire environment. Formally, let \( \mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_R \) be \( R \) disjoint fragments of the environment, \( \mathcal{F}_i \cap \mathcal{F}_j = \emptyset \) for \( i \neq j \). Then,

\[
R_\delta(A) = \max_{\{\mathcal{F}_j\}} \left\{ R : \hat{I}_{\mathcal{F}_j}(A) \geq (1 - \delta)\hat{I}_E(A), \forall j = 1, \ldots, R \right\} \tag{2.12}
\]

where the maximization is carried over all partitions of \( \{\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_N\} \) into disjoint subsets. Clearly, for any observable \( A \), \( 1 \leq R_\delta(A) \leq N \). Redundancy simply counts the number of copies of the imprint of \( A \) in \( \mathcal{E} \), without judging the quality of their information content. Indeed, \( \hat{I}_E(A) \) and \( R_\delta(A) \) play two very distinct roles. It is possible for example that \( \mathcal{E} \) contains very little information about \( A \), so \( \hat{I}_E(A) \ll H(A) \), but that this information is perfectly imprinted many times in \( \mathcal{E} \), so \( R_{\delta=0}(A) \gg 1 \). Another possibility is that the whole environment contains a perfect imprint of \( A \), \( \hat{I}_E(A) = H(A) \), while individual fragments contain a poor imprint \( I_{\mathcal{F}}(A) \ll H(A) \). In this case, the number of good imprints of the information is very low \( R_{\delta=0}(A) \approx 1 \), the number of bad imprints can of course still be high \( R_\delta(A) \gg 1 \) only for \( \delta \approx 1 \).

**Fragments of the environment and elementary subsystems**

Before closing this section, we wish to emphasize the distinction we are making between fragments of \( \mathcal{E} \) and elementary subsystems, and comment on the role they play in using environment as a witness. The elementary subsystems of \( \mathcal{E} \) are defined through the natural tensor product structure of \( \mathcal{H}\mathcal{E} \). We assume this structure to be given and fixed. In the case of a photon environment for instance, an elementary subsystem could consist of a single photon. A fragment of \( \mathcal{E} \) on the other hand is a collection of such elementary subsystems. For example, while no single photon can reveal the position of an object, a small collection of them, say 1000, may be enough to do so.
The optimization over partitions of the environment appearing at Eq. (2.12) is necessary to arrive at a proper mathematical definition of redundancy as there is no a priori preferred partition. This will allow us to derive very general consequences of redundancy, at the price of some technical (and perhaps also conceptual) complications. However, for the purposes of the emergence of a consensus among several observers — in essence an operational objective reality — this partition should reflect the distinct fragments of environment accessible to the different observers. While our results hold for any such partition of the environment into disjoint subsystems, Nature ultimately determines what part of $E$ is available to each observer.

The entire environment as a witness approach — and more precisely the very concept of redundancy — capitalizes on the fact that the environment has a tensor product structure $\mathcal{H}_E = \bigotimes_{E_k} \mathcal{H}_{E_k}$. This raises the obvious question “who decides what are the elementary subsystems of $E$?” We see two different aspects of this issue, each leading to a separate answer.

Our primary concern here is to provide a mechanism by which quantum systems can exhibit “objective existence”, the key symptom of the classical behavior. As we will demonstrate, this can be achieved given that the environment has a partition into subsystems, regardless of what these subsystems are. Hence, what really matters is that various observers monitor different fragments of the environment. Section 2.5 will present unavoidable consequences of this fact, without paying attention to the definition of the environmental subsystems. Thus, our most important conclusion, that redundancy implies selection of a preferred observable, is independent of any particular choice of a tensor product in the environment.

However, different tensor product structure of the environment can a priori yield different redundantly imprinted observables since redundancy itself makes reference to the tensor product structure. Thus, to pursue environment as a witness program in the future, and in particular to identify the preferred observables in specific models, we will need to address this issue. There is no definite answer to what defines an elementary environmental subsystem, but some considerations point towards “locality” as a judicious guideline.

For instance, particles are conventionally defined by the symmetries of the fundamental Hamiltonians of Nature (in particular Lorentz invariance), that are local. When we choose the particles of the standard model as the elementary subsystems, we are
therefore naturally led to local couplings between $S$ and $E$. They will determine how the information is inscribed in $E$. Moreover, the information acquisition capacities of the observers are also ultimately limited by the fundamental Hamiltonians of Nature. The different observers occupy, and therefore monitor, different spatial regions. Therefore, the monitored fragments $F_i$ entering in the definition of redundancy — as well as the elementary subsystems $E_k$ composing them — should reflect these distinct spatial regions.

The fact that some division of the Universe subsystems is needed has been pointed out before. Indeed, the measurement problem disappears when the Universe cannot be divided into subsystems [Zur93b, Zur03a, Sch03a]. Therefore, assuming that some such division exists in the discussion of the information-theoretic aspects of the origin of the classical does not seem to be a very costly assumption (and has indeed been employed in several discussions of the foundations of quantum mechanics, e.g. [GRW86a, Die96a, Leg02a]).

2.5. Consequences of redundancy

We now have all the necessary ingredients to study the consequences of the existence of redundant information about the system in the environment. Here, we derive several properties of the system’s redundantly imprinted observables, as well as properties of the environmental observables revealing this information. While each of these results are interesting in their own right, our ultimate goal is to combine them into the main theorem of this section, which essentially ensures the uniqueness of redundantly imprinted observables. Throughout this section, we assume the existence of a perfect and redundant record of the system observables $A, B, C, \ldots$ in the environment, i.e. $\hat{I}_{E}(A) = H(A)$ and $R_{\delta=0}(A) \gg 1$, and similarly for $B, C, \ldots$ The general case of imperfect imprints will be addressed in the next section. Let us begin by studying the consequences of the existence of a record about the value of $A$ in the environment.

**Lemma 2.5.1.** When $\hat{I}_{E}(A) = H(A)$, there exists an observable $\hat{X} \in \mathcal{M}_{E}$ for which $H(A|\hat{X}) = 0$ and $H(\hat{X}|A) = 0$; the measurement of $\hat{X}$ on a fragment of the environment reveals all the information of the system observable $A$, and vice and versa.

**Proof** When observable $A$ is completely encoded in a fragment of the environment, $\hat{I}_{E}(A) = H(A)$, there exists $X \in \mathcal{M}_{E}$ for which $I(A : X) = H(A)$. As mentioned
in Section 2.4.1, the mutual information between $A$ and $X$ is symmetric when these observables act on distinct systems, i.e. $S$ and $F$. Therefore, measuring $A$ directly on the system provides an amount of information $I(A : X) = H(A)$ about the value of $X$, thereby decreasing its entropy to $H(X | A) = H(X) - H(A)$. In general, this is not all the information about $X$, as $H(X)$ may be larger than $H(A)$: $X$ reveals all of the information about $A$ but the reverse is in general not true. However, by picking a suitable coarse graining $\tilde{X}$ of $X$, it is always possible establish the duality $H(A | \tilde{X}) = 0$ and $H(\tilde{X} | A) = 0$.

This can be seen quite simply. The equality $H(A | X) = 0$ implies that given $X_j$, $A_i$ is determined: each measurement outcome of $X$ points to a unique measurement outcome of $A$. This defines a map $f : \{X_j\} \rightarrow \{A_i\}$. Such map may not be one-to-one, so the conditional probability $P(X_j | A_i)$ of $X_j$ given $A_i$ is not necessarily deterministic. However, we can construct the coarse grained projectors

$$\tilde{X}_i = \sum_{j : f(X_j) = A_i} X_j$$

(2.13)

by regrouping the $X_j$ in the pre-image of $A_i$. The outcome of the associated measurements $\tilde{X}$ are therefore in one-to-one correspondence to the outcomes of $A$, yielding the stated duality.

An important corollary can be derived from Lemma 2.5.1 and the following observation: when the outcome of a projective measurement on a system is deterministic, the act of measuring does not modify the state of the system.

**Corollary 2.5.1.** Measurements of $A$ and $\tilde{X}$ have exactly the same effect on the joint state of the system and the environment:

$$\tilde{X}_j \rho^{SE} \tilde{X}_j = A_j \tilde{X}_j \rho^{SE} \tilde{X}_j A_j = A_j \rho^{SE} A_j,$$

(2.14)

which implies $\rho^{SE}_{|X_j} = \rho^{SE}_{|A_j}$.

The content of Lemma 2.5.1 and Corollary 2.5.1 formalizes our intuitive understanding of the existence of a perfect record of the information about $A$ in $E$: it allows perfect emulation of the direct measurement $A$ by the indirect measurement $\tilde{X}$. This emulation is not only perfect from the point of view of its information yield, it also has the same physical effect on the state of $SE$. This can be regarded as an illustration of the
fact that “information is physical” [Lan91a]: whenever the same information can be retrieved by two different means, the disturbance on the quantum state can be identical. Moreover, this corroborates the idea that quantum states represent our information about the system. Here, the measurement of $X$ can in principle yield more information than the direct measurement $A$ itself, e.g. $A$ may be a very coarse grained observable. This is why it is in general necessary to coarse grain $X$ in order to obtain equivalent information, and therefore the same physical effect.

**Lemma 2.5.2.** When $I_F(A) = H(A)$, the observable $A$ commutes with the reduced density matrix of the system, $[\rho^S, A] = 0$.

**Proof** Following Lemma 2.5.1 and Corollary 2.5.1, there exists $\tilde{X} \in \mathcal{E}$ for which $\tilde{X}_j \rho^{SE} \tilde{X}_j = A_j \rho^{SE} A_j$. The reduced state of the system can be therefore written as

$$
\rho^S = \text{Tr}_E \{ \rho^{SE} \} = \sum_j \text{Tr}_E \{ \tilde{X}_j \rho^{SE} \tilde{X}_j \}
$$

$$
= \sum_j \text{Tr}_E \{ A_j \rho^{SE} A_j \} = \sum_j A_j \rho^S A_j,
$$

so $\rho^S$ is block diagonal in the eigensubspaces of $A$.

The relation between decoherence and the existence of an environmental record has been pointed out and investigated in the past [Zur81a, Zur82a, Zur83a, Zur93b, GJK+96a, GH97b, Zur98a, Hal99b]. The above lemma confirms that whenever the environment acquires a single copy of the information about $A$, the state of $S$ decoheres with respect to the spectral projectors $A_i$ of $A$. This decoherence-induced diagonalization of the reduced state has an important consequence when the information about the system is encoded redundantly in the environment.

**Corollary 2.5.2.** Let $A$ be a system observable redundantly imprinted in $\mathcal{E}$, and let $\tilde{X}$ be the coarse grained observable acting on the fragment $F$ of the environment that reveals all the information about $A$ (as constructed in Lemma 2.5.1). Then the reduced state $\rho_{SF}$ commutes with both $A$ and $\tilde{X}$: the correlations between these observables are classical.

---

1In the theory of generalized measurements [Kra83a], one can in principle make a measurement that yields no information whatsoever, yet greatly disturb the system; hence the emphasized “can” in the above sentence.
2.5. Consequences of redundancy

Proof Since $A$ is redundantly imprinted in $\mathcal{E}$, its value can be inferred by independent measurements, say $X$ and $Y$, acting on at two distinct fragments of the environment, $\mathcal{F}$ and $\mathcal{F} = \mathcal{E} - \mathcal{F}$ respectively. Following Lemma 2.5.1, we can construct a coarse grained observable $\tilde{X}$ which retains essential correlations to $A$ and with the property that $H(\tilde{X}|A) = 0$ — a measurement of $A$ on $S$ reveals all the information about $\tilde{X}$. As a consequence, the measurement $Y$ on $\mathcal{F}$ that reveals all the information about $A$ must also reveals all the information about $\tilde{X}$. Hence, Corollary 2.5.2 follows from Lemma 2.5.2.

We will now characterize the class of system observables that can be redundantly imprinted in the environment. When $A$ and $B$ are redundantly imprinted in $\mathcal{E}$ and redundancy is sufficiently high, their value can be inferred from disjoint fragments of the environment. This implies the following relation between any redundantly imprinted observables.

Lemma 2.5.3. Let $\mathcal{F}$ be a fragment of the environment containing a copy of the information about $A$. When the rest of the environment $\mathcal{F}$ contains a copy of the information about $B$, then $A$ and $B$ necessarily commute on the support of $\rho^S$.

Proof The assumptions of Lemma 2.5.3 imply the existence of two environmental observables $X$ and $Y$ acting on disjoint fragments of the environment $\mathcal{F}$ and $\mathcal{F}$ for which $H(A|X) = 0$ and $H(B|Y) = 0$. Following the procedure of Lemma 2.5.1, we can coarse grain these two observables into $\tilde{X}$ and $\tilde{Y}$ that are in one-to-one correspondence with $A$ and $B$ respectively. The observables $\tilde{X}$ and $\tilde{Y}$ obviously commute with each other as they act on disjoint fragments of $\mathcal{E}$, and also commute with the system observables $A$ and $B$. Then, by Corollary 2.5.1, we have

$$A_iB_j\rho^{S\mathcal{E}}B_jA_i = A_i\tilde{Y}_j\rho^{S\mathcal{E}}\tilde{Y}_jA_i = \tilde{Y}_jA_i\rho^{S\mathcal{E}}A_i\tilde{Y}_j = \tilde{Y}_j\tilde{X}_i\rho^{S\mathcal{E}}\tilde{X}_i\tilde{Y}_j,
$$

$$\tilde{X}_iB_j\rho^{S\mathcal{E}}B_j\tilde{X}_i = B_j\tilde{X}_i\rho^{S\mathcal{E}}\tilde{X}_iB_j = B_jA_i\rho^{S\mathcal{E}}A_iB_j,$$

proving the lemma.

The above Lemma states that it is impossible to acquire perfect information about two non-commuting observables by measuring two distinct fragments of $\mathcal{E}$ simultaneously. This is reminiscent of Heisenberg indeterminacy principle. However, in spite
Environment as a witness

of their similarity, these two results differ in the precise setting in which they hold. Heisenberg principle asserts that it is impossible to know simultaneously the values of two non-commuting observables of an otherwise isolated system. In our Lemma, the system is already correlated with its environment, and the observer is trying to find out about the value of two observables using these correlations. In other words, Heisenberg indeterminacy concerns information about the system before it interacted with $\mathcal{E}$, while Lemma 2.5.3 focuses to the information about $S$ that is present in $\mathcal{E}$ after their interaction.

To fully grasp the distinction between these two settings requires a somewhat technical discussion. Assume that the system and environment are initially in the uncorrelated state $\rho^{SE}(0) = \rho^S(0) \otimes \rho^E(0)$. They interact for a time $t$, yielding the joint state $\rho^{SE}(t) = U^{SE} \rho^{SE}(0) U^{SE\dagger}$ where $U^{SE} = \exp\{-iH^{SE}t\}$. When a measurement $X$ is carried on the environment and outcome $j$ is observed, the conditional state of the system will be

$$\rho^S_{|X_j}(t) = \frac{\text{Tr}_E \{X_j \rho^{SE}(t) X_j\}}{p(X_j)}.$$

According to the generalized theory of measurement [Kra83a], this can be described as a positive operator valued measure (POVM) acting on the initial state of the system, $\rho^S(0)$. Formally, there exists a set of operators $A_{ij}$ acting on $\mathcal{H}^S$ such that $\rho^S_{|X_j}(t) = \sum_i A_{ij} \rho^S(0) A_{ij\dagger}$. However, it does not correspond to any kind of measurement acting on $\rho^S(t)$, the state of the system after it has interacted with $\mathcal{E}$ (see for example [Fuc02c] Eq. (100)). Our Lemma applies also to this type of information gathering processes that cannot be described within the POVM formalism.

This difference illustrates the specificity of our operational approach: we are describing the physical properties of an open quantum system, hence we focus on information about its present state, not on what it was prior to the interaction with $\mathcal{E}$. Decoherence happens unavoidably, so we are dealing with it.

We can derive a similar result for the commutation of environmental observables.

**Lemma 2.5.4.** Let $\mathcal{F}$ be a fragment of the environment containing information about both $A$ and $B$, two commuting system observables. Then, there exist two observables $\tilde{X}$ and $\tilde{Y} \in \mathcal{M}_\mathcal{F}$ that commute on the support of $\rho^{SE}$ and reveal all the information about $A$ and $B$ respectively.
Proof The assumptions of Lemma 2.5.4 imply the existence of $X$ and $Y \in M$ such that $I(A : X) = H(A)$ and $I(B : Y) = H(B)$. Following the procedure of Lemma 2.5.1, $X$ and $Y$ can be coarse grained to $\tilde{X}$ and $\tilde{Y}$ while retaining all the essential correlations to $A$ and $B$. Since $A$ and $B$ commute, the proof of Lemma 2.5.3 can be applied here, yielding the desired result.

Given these properties of redundantly imprinted observables, we can now state a very important result, which essentially ensures the uniqueness of redundantly imprinted observables.

**Theorem 2.5.1.** Let $B$ and $C$ be two system observables redundantly imprinted in the environment, and let $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_R$ be $R$ disjoint fragments of $E$, each containing a copy of the information about $B$ and $C$. Then, there exists a refined system observable $A$ satisfying:

1. $\hat{\mathcal{I}}_E(A) = H(A)$,
2. $R_{d=0}(A) \geq R$,
3. $H(B|A) = 0$ and $H(C|A) = 0$.

Proof The assumptions of the theorem imply the existence of $Y^{\mathcal{F}_n}$ and $Z^{\mathcal{F}_n} \in M_{\mathcal{F}_n}$ for which $H(B|Y^{\mathcal{F}_n}) = 0$ and $H(C|Z^{\mathcal{F}_n}) = 0$ for all $n = 1, \ldots, R$. By Lemma 2.5.3, $B$ and $C$ must commute as they can be inferred from disjoint fragments of the environment. This fact, together with Lemma 2.5.4, implies that there exists commuting coarse grained observables $\hat{Y}^{\mathcal{F}_n}$ and $\hat{Z}^{\mathcal{F}_n} \in M_{\mathcal{F}_n}$ that reveal all of the information about $B$ and $C$ respectively. The observables $B$ and $C$ can be merged into a more refined observable $A$ with spectral projectors given by the product of the spectral projectors of $B$ and $C$:

$$A_{ij} = B_i C_j. \quad (2.18)$$

As $B_i$ and $C_j$ commute, the operators $A_{ij}$ form a complete set of mutually orthogonal projectors. Similarly, the environment observables $\hat{Y}^{\mathcal{F}_n}$ and $\hat{Z}^{\mathcal{F}_n}$ can be merged into a more refined observable $X^{\mathcal{F}_n}$ with spectral projectors $X_{ij}^{\mathcal{F}_n} = \hat{Y}_i^{\mathcal{F}_n} \hat{Z}_j^{\mathcal{F}_n}$. A measurement
Environment as a witness

of \( X_{\mathcal{F}_n} \) on \( \mathcal{F}_n \) reveals all the information about \( A \). Indeed, following Corollary 2.5.1,

\[
P(A_{ij'}|X_{ij}^{\mathcal{F}_n}) = \frac{\text{Tr} \left\{ A_{ij'} X_{ij}^{\mathcal{F}_n} \rho_{\mathcal{SE}} X_{ij}^{\mathcal{F}_n} A_{ij'} \right\}}{\text{Tr} \left\{ X_{ij}^{\mathcal{F}_n} \rho_{\mathcal{SE}} X_{ij}^{\mathcal{F}_n} \right\}}
\]

which implies \( H(A|X_{\mathcal{F}_n}) = 0 \). This automatically implies \( \hat{I}_{\mathcal{F}_n}(A) = H(A) \) and, since the above holds for all \( n = 1, \ldots R \), we have \( R_0(A) \geq R \). Finally, note that \( B_i = \sum_j A_{ij} \) and \( C_j = \sum_i A_{ij} \); \( B \) and \( C \) are obtained by coarse graining \( A \). Therefore, a measurement of \( A \) reveals all the information about \( B \) and \( C \), hence completing the proof.

The meaning of this theorem is that whenever more than one observable can be redundantly inferred from disjoint fragments of \( \mathcal{E} \), they necessarily correspond to some coarse grained version of a \textit{maximally refined redundantly imprinted observable} \( A \). This proves our claim of Section 2.2 that redundant spreading of information comes at the price of singling out a preferred system observable \( A \). The \textit{modus tollens} of this Theorem is also very enlightening. Given the maximally refined redundantly imprinted observable \( A \), the only observables \( B \) that can be completely and redundantly imprinted in the environment are those for which \( I(B : A) = H(B) \); the value of \( B \) must be entirely determined by a measurement of \( A \). This is obviously a sufficient condition: if a direct measurement of \( A \) reveals all the information about \( B \) and \( A \) is redundantly imprinted in \( \mathcal{E} \), then so is \( B \). Theorem 2.5.1 shows that this requirement is also necessary.

So far, we have not considered any dynamical evolution of the system and environment: we have focused on the correlations present at a fixed time without paying attention to how they arise. We studied consequences of regarding environment as a witness (and interrogating it about the state of the system), but we haven’t yet enquired about the dynamics that allowed the environment to acquire this information in the first place. Ultimately, it is the coupling Hamiltonian between \( \mathcal{S} \) and \( \mathcal{E} \) which establishes these correlations. In conventional approaches to decoherence, the coupling is also responsible for the emergence of a preferred system observable — the pointer observable — that is least affected by the openness of the system. Thus, the connection
between the emergence of an objective reality and the selection of a preferred observable can only be established through dynamical considerations. When the correlations between the maximally refined observable and fragments of the environment persist in time, Lemma 2.5.2 and Theorem 2.5.1 imply the following conclusion.

**Corollary 2.5.3.** The maximally refined redundantly imprinted observable $A$ is the system’s pointer observable.

In other words, only the already familiar pointer observable can leave a redundant and robust imprint on $E$. Corollary 2.5.3 can be understood as a consequence of the ability of the pointer states to persist while immersed in the environment. This resilience allows the information about the pointer observables to proliferate, very much in the spirit of the Darwinian “survival of the fittest”. This, along with other facts, will be illustrated on a dynamical model in the next section.

### 2.6. Quantum Darwinism: Dynamical emergence of objectivity

It should by now be clear that the presence of redundant information in the environment imposes severe physical constraints on the state of the system. Surprisingly, the derivation of these important facts required little physics — most of them followed from information-theoretic arguments, once again illustrating that information is physical. While all the results of Section 2.5 are universally true, we must now demonstrate that our starting point — namely the existence of redundant information in $E$ — can indeed occur in the real world. We will show that realistic physical models can produce a redundant imprint of the properties of $S$ in the environment.

Moreover, focusing on the dynamics of $SE$ rather than on their state will allow us to extend our analysis. In particular, we will show that when the imprints of the objective observable are nearly perfect — i.e. $\hat{I}_E(A) \geq (1 - \vartheta)H(A)$ and $R_\delta(A) > 1$ for $\vartheta$ and $\delta$ finite but small — the conclusions obtained earlier still hold. Above all, along the lines of Theorem 2.5.1, there exists a unique maximally refined observable whose information is the only one available in fragments of $E$. Finally, we will be able to specify the optimal measurement to be performed on fragments of $E$ to learn about the system. This is a considerable improvement over the result of the last section where, in the absence of any model Hamiltonian, we could only demonstrate the existence of such a measurement. Hence, this section is an extension of our general analysis.
Dynamics of Quantum Darwinism and decoherence

The model we consider is a generalization of the simple early model of decoherence put forward in [Zur82a] and thoroughly investigated as a simple, yet nontrivial, paradigm for decoherence: despite its simplicity, it captures the essence of einselection. Hence, our simple model serves as a “case-study” that sets a good conceptual framework for the study of more sophisticated models, such as a photon environment scattering on an object and carrying away potential visual data. As any specific model, it requires some fairly specific assumptions. We shall consider their role in Section 2.7: we will see there the extent to which relaxing some of these assumptions affects our conclusions.

A system $S$ is coupled to an environment $E = \{E_1, E_2, \ldots\}$ through the Hamiltonian:

$$H^{SE} = \sum_{E_k \in E} A \otimes Z^{E_k},$$

(2.19)

where $A$ and $Z^{E_k}$ are operators acting on $S$ and $E_k$ respectively. The joint initial state of the system and the different environmental subsystems is assumed to be a pure product state:

$$|\Phi_{SE}(0)\rangle = |\phi_S\rangle \otimes |\phi_{E_1}\rangle \otimes |\phi_{E_2}\rangle \otimes \ldots.$$  

(2.20)

Hence, before the interaction, there is no correlation between the system and the environment, nor among the environmental subsystems.

A convenient way of writing $|\phi_S\rangle$ in view of expressing the time evolution of the joint state of $SE$ is to decompose it in an eigenbasis $|i\rangle$ of $A$ ($A|i\rangle = a_i|i\rangle$):  

$$|\phi_S\rangle = \sum_i \alpha_i |i\rangle.$$  

(2.21)

Without loss of generality, we can assume that the vectors $|i\rangle$ with non-zero coefficients $\alpha_i$ in Eq. (2.21) are associated with distinct eigenvalues $a_i$ of $A$. This can be done by choosing appropriate bases for the degenerate eigenspaces of $A$. Thus, after an interaction time $t$ with the $N$ subsystems of the environment, the joint state of $SE$ evolves into:

$$|\Phi_{SE}(t)\rangle = \sum_{j} \alpha_j |j\rangle \bigotimes_{E_k \in E} e^{-ia_j Z^{E_k} t} |\phi_{E_k}\rangle$$

$$= \sum_{j} \alpha_j |j\rangle \bigotimes_{E_k \in E} |\phi^E_{j\rangle},  

(2.22)

(2.23)
where we have defined $|\phi_j^{E_k}\rangle = e^{-ia_jZ^{E_k}t}|\phi_k^{E_k}\rangle$.

In the following sections, we will analyze the correlations between the system $S$ and the “observed” part of the environment $F$. For example, in the case of a photon environment scattering on an object, $F$ is the set of photons that hit the observer’s retina, while $\bar{F}$ represents those photons that have scattered on $S$ but that are not intercepted by the observer. Equation (2.23) allows us to compute the state of $S$ and $F$:

$$\rho^{SF} = \sum_{ij} \alpha_i \alpha_j^* |i\rangle \langle j| \otimes |\Phi_j^F\rangle \langle \Phi_i^F| \times \gamma_{ij}^F,$$

where

$$|\Phi_j^F\rangle = \bigotimes_{E_k \in F} e^{-ia_jZ^{E_k}t}|\phi_k^{E_k}\rangle = \bigotimes_{E_k \in F} |\phi_j^{E_k}\rangle,$$

and $\gamma_{ij}^F = \prod_{E_k \in \bar{F}} \langle \phi_j^{E_k}|\phi_i^{E_k}\rangle = \langle \Phi_j^F|\Phi_i^F\rangle$. Similarly, the reduced state of the system at time $t$ reads:

$$\rho^S = \sum_{ij} \alpha_i \alpha_j^* |i\rangle \langle j| \times \gamma_{ij}^E,$$

where $\gamma_{ij}^E = \prod_{E_k \in E} \langle \phi_j^{E_k}|e^{-i(a_i - a_j)Z^{E_k}t}|\phi_i^{E_k}\rangle$. Above, the $\gamma$’s are called the *decoherence factors*.

Except in carefully controlled experiments — where the system can be very well isolated from its environment — the number of environmental subsystems interacting with $S$ is huge. In this case, the $\gamma_{ij}^E$’s will be typically very small for $i \neq j$. Each environmental subsystem contributes a factor $\langle \phi_j^{E_k}|e^{-i(a_i - a_j)Z^{E_k}t}|\phi_i^{E_k}\rangle$ to $\gamma_{ij}^E$, so unless $|\phi_k^{E_k}\rangle$ is an eigenstate of $Z^{E_k}$ — in which case $E_k$ is effectively decoupled from the system — this strictly decreases the decoherence factor. Hence, $\gamma_{ij}^E$ goes to $\delta_{ij}$ as $N$ increases. To be more specific, when the initial states of the environmental subsystems are distributed uniformly at random, the decrease of $\gamma_{ij}^E$ is exponential with $N$ and typically Gaussian with time [ZCP03a].

This reasoning also applies to the decoherence factors $\gamma_{ij}^F$: they tend to zero (for $i$ not equal to $j$ as the number of unobserved environmental subsystems increases. Even though a considerable number of the environmental subsystems can be intercepted by the observer, an even larger fraction will usually escape his monitoring. Thus, the $\gamma_{ij}^F$’s will also typically be very small for $i \neq j$. 
**Decoherence: the focus on the system**

In order to contrast the environment as a witness approach to classicality as well as to illustrate significance of the dynamics that leads to quantum Darwinism, we will now review some results that were obtained using more conventional approaches. Thus, immediately below we will for the moment abandon the study of correlations between $S$ and parts of the environment to focus uniquely on the state of the system, as it is done in the the standard studies of decoherence [GJK+96a, PZ01a].

We see from Eq. (2.26) that the off-diagonal terms of the system’s density matrix tend to be very small when expressed in the $|i\rangle$ basis. It is therefore natural to expect that these are the quasi-classical states of the system: the coupling to the environment suppresses quantum superpositions of the states $|i\rangle$. Of course, the exact diagonal basis of $\rho^S$ might be significantly different from $|i\rangle$, especially when the coefficients $\alpha_j$ of the system’s initial state Eq. (2.21) are almost equal. Hence, for someone focused on the instantaneous state of the system, it may not be clear why the basis $|i\rangle$ deserves any special attention in spite of the existence of small — yet non-zero — off-diagonal elements for $\rho^S$. However, a simple analysis shows that the basis $|i\rangle$ is the only basis for which all off-diagonal terms tend to zero independently of the initial state of the system [Zur03a, Sch03a]. This persistence is a very important property of the to-be-classical states: the emergence of an objective quasi-classical domain must be independent of the subjective initial state of the system.

Moreover, when the system is initially prepared in one of the states $|i\rangle$, it will not be affected by the interaction with the environment: pointer states are stable. In more general cases (more complicated interactions, etc.), the above simple analysis cannot be carried out, and one usually relies on the predictability sieve [Zur93b, ZHP93a, GJK+96a, PZ01a] that implements the same idea — defining classical existence through persistence of correlation, and hence, through predictability — to find the pointer basis. Predictability sieve seeks most predictable initial states — states that produce the smallest amount of entropy over time while subject to interaction with the environment.

**Perfect correlations**

We now return to the study of the correlations between $S$ and fragments of the environment. Our goal is to characterize how and what kind of information is stored in the
environment when it is redundant. To be more precise, we will analyze the structure of information in a fragment $\mathcal{F}$ of $\mathcal{E}$ under the assumption that the rest of the environment, i.e. $\mathcal{F} = \mathcal{E} - \mathcal{F}$, contains at least another copy of this information. Our demand that both $\mathcal{F}$ and $\mathcal{F}$ contain a copy of the information insures a minimum redundancy of $R \geq 2$ which — although insufficient to ensure the emergence of a consensus about the properties of $S$ among many observers — is enough to re-derive directly all the results established in Section 2.5, i.e. to illustrate the unavoidable consequences of redundant imprinting. In addition, we will be able to specify optimal measurement strategies on $\mathcal{F}$, the fragment of $\mathcal{E}$ accessible to the observer, for inferring any kind of information about $S$.

To build our intuition, it is enlightening to first consider the limiting case $\gamma_{ij}^{\mathcal{F}} = \delta_{ij}$, where $\gamma_{ij}^{\mathcal{F}} = \langle \Phi_i^{\mathcal{F}} | \Phi_j^{\mathcal{F}} \rangle$. We return to the general case in Section 2.6.4. Following the general argument of Section 2.6.1, this condition reflects the physical assumption that both the observed and the unobserved fragments of $\mathcal{E}$ are very large. For obvious reasons, we call these correlations perfect. Under such assumption, the density matrix of $S$ and $\mathcal{F}$ reads

$$\rho_{SF} = \sum_i |\alpha_i|^2 |i\rangle \langle i| \otimes |\Psi_i^{\mathcal{F}}\rangle \langle \Psi_i^{\mathcal{F}}|$$

(2.27)

where the $|\Psi_i^{\mathcal{F}}\rangle$’s are mutually orthogonal. Note that the $|\Phi_i^{\mathcal{F}}\rangle$’s of Eqs. (2.24-2.25) have been replaced by $|\Psi_i^{\mathcal{F}}\rangle$’s to emphasize that $\langle \Psi_i^{\mathcal{F}} | \Psi_j^{\mathcal{F}} \rangle = \gamma_{ij}^{\mathcal{F}} = \delta_{ij}$. Similarly $\rho$ has been replaced by $\rho_{SF}$.

Consider the observable $X \in M_\mathcal{F}$ that perfectly distinguishes between the orthogonal states $|\Psi_i^{\mathcal{F}}\rangle$:

$$X = \sum_i x_i |\Psi_i^{\mathcal{F}}\rangle \langle \Psi_i^{\mathcal{F}}| = \sum_i x_i X_i.$$  

(2.28)

Following Eq. (2.5), the state of the system after a measurement of $X$ on $\mathcal{F}$ with outcome $X_j$ is

$$\rho_{X_j}^S = \text{Tr}_\mathcal{F} (\rho_{SF}^{X_j}) = \frac{\text{Tr}_\mathcal{F} \{ X_j \rho_{SF}^{X_j} X_j \} }{P(X_j)} = |j\rangle \langle j|.$$  

(2.29)

This is the same as the state of $S$ after a direct measurement of $A$ with outcome $A_j$, $\rho_{A_j}^S = \rho_{A_j}^S$. Thus, a subsequent measurement of $A$ on the system yields outcome $A_i$ with certainty, so $H(A | X) = 0$. The same conclusion can be reached for a measurement acting on $\mathcal{F}$: thus, $A$ is encoded redundantly in $\mathcal{E}$ (there are at least two copies). As
a consequence, all the results of Section 2.5 trivially hold. It is however instructive to
derive them directly for our specific model, without appealing to the general lemmas.

As seen from Eq. (2.29), the indirect measurement $X$ perfectly emulates the direct
measurement $A$ on the system. Consequently, all the information about the observable
$A$ can be extracted by the measurement $X$ on the environment. In addition, we clearly
see the “no-information / no-disturbance” principle at work: once the outcome of $X$ is
known, measuring $A$ directly does not disturb the state of the system any further, as
the measurement of $X$ “projects” the system in an eigenstate of $A$ (see Corollary 2.5.1).
Averaging over the measurement outcomes of $X$ yields the reduced density matrix of
$S$, which is accordingly a mixture of the eigenstates of $A$, so $[\rho^S, A] = 0$ as specified by
Lemma 2.5.2.

Specifying the Hamiltonian responsible for the correlations between $S$ and its envi-
nronment allows us to go beyond the purely information-theoretic analysis of Section 2.5.
Given the explicit form of the density matrix $\rho^{SF}$, we can address more interesting
questions such as: what is the optimal measurement $Y$ on $F$ that yields the largest
amount of information about a given system observable $B$? In fact, it turns out that
$X$ is the optimal measurement on $F$ to find out the value of any system observable $B$.
Regardless of what we wish to learn about the system, the optimal strategy consists in
measuring $X$ on $F$:

$$I(B : X) \geq I(B : Y)$$

for all $B \in M_S$ and $Y \in M_F$. Similarly, when a non-optimal measurement $Y$ is carried
on $F$, it is always primarily correlated with the pointer observable $A$. In other words,
when a measurement $Y$ is carried on a fragment of the environment, it always reveals
more information about the pointer observable $A$ than any other system observable:

$$I(A : Y) \geq I(B : Y)$$

for all $B \in M_S$ and $Y \in M_F$.

Let us prove these two very important assertions. First, note that following Eqs. (2.8,2.10),
the mutual information between any system observable $B$ and environmental observable
$Y$ takes the following form:

$$I(B : Y) = H(B) - H(B|Y)$$

$$= H(Y) - H(Y|B).$$
2.6. Quantum Darwinism: Dynamical emergence of objectivity

When \( B \) is a fixed system observable, maximizing \( I(B : Y) \) amounts to minimizing \( H(B|Y) \). To do this, consider the conditional state \( \rho_{SY}^{B|Y} \) of the system given a measurement outcome \( Y_i \) on \( F \). Simple algebraic manipulations can be used to show that

\[
\rho_{SY}^{B|Y} = \text{Tr}_F \{ Y_i \rho_{SF}^{B|Y} \} \quad \text{with} \quad P(Y_i) = \sum_j P(X_j|Y_i) \rho_{S|X_j}.
\]

(2.34)

We see that \( \rho_{SY}^{B|Y} \) is a convex combination of the \( \rho_{S|X_j} \). (This is no algebraic coincidence: it follows from Corollary 2.5.1, Lemma 2.5.3, and the existence of information about \( A \), and hence about \( X \), in the rest of the environment \( \overline{F} \).) Hence, the inequality of Eq. (2.30) follows from the convexity of entropy, c.f. Proposition A.0.4. Similarly, when \( Y \) is a fixed measurement on \( F \), maximizing \( I(B : Y) \) amounts to minimizing \( H(Y|B) \).

We can consider the state of \( F \) following a measurement of \( B \) on \( S \)

\[
\rho_{B}^{F} = \text{Tr}_S \{ B_i \rho_{SF}^{B|i} \} \quad \text{with} \quad P(B_i) = \sum_j P(A_j|B_i) \rho_{A|B}^{F}.
\]

(2.35)

a convex combination of the states of \( F \) conditioned on a measurement of \( A \) on \( S \). Again, the inequality Eq. (2.31) follows from convexity of entropy, c.f. Proposition A.0.4.

By combining Eq. (2.30) with the fact that measuring \( X \) perfectly emulates the direct measurement \( A \) on \( S \), we get the following equality:

\[
\hat{I}_F(B) = I(B : A),
\]

(2.36)

the information about \( B \) accessible from the fragment \( F \) is inherently limited by its correlation with the maximally refined observable \( A \). The only assumption required to arrive at this important equality is that correlations with both the observed and the unobserved parts of the environment impose \( \gamma^{F}_{ij} = \gamma^{\overline{F}}_{ij} = \delta_{ij} \). This requirement is, according to Corollary 2.5.2, equivalent to saying that both \( F \) and \( \overline{F} \) contain a perfect copy of the information about \( A \).

The consequences of Equation (2.36) can be better appreciated once we recognize that it allows us to evaluate the redundancy for any system observable straightforwardly. When the value of \( B \) can be deduced from knowledge of the value of \( A \), then each fragment of \( E \) containing information about \( A \) will inevitably contain information about \( B \). Formally,

\[
I(B : A) \geq (1 - \delta) \hat{I}_E(B) \Rightarrow R_{\delta}(B) \geq R_{\delta=0}(A).
\]

(2.37)
On the other hand, when the value of $B$ cannot be deduced from knowledge of $A$, $B$ cannot be redundant. Formally,

$$I(B : A) < (1 - \delta)I_{\bar{\mathcal{E}}}(B) \Rightarrow R_\delta(B) = 1.$$  

(2.38)

Indeed, whenever a fragment $\mathcal{F}$ of $\mathcal{E}$ is sufficiently large to reveal information about $B$, the discussion following Eq. (2.36) implies that the rest of the environment $\mathcal{F}$ is too small to contain the information about $A$, and hence, following Eq. (2.36), cannot contain information about $B$.

Note that these results can also be derived with the help of the data processing inequality (see Proposition A.0.5). In effect, the update rule of Eq. (2.5) shows that the sequence of measurements $B, A, X, Y$ forms a Markov chain ($B$ and $Y$ are arbitrary): the joint probability of the measurement results of $B, A, X, Y$ satisfies

$$P(Y_i, X_j, A_k, B_l) = P(Y_i|X_j)P(X_j|A_k)P(A_k|B_l)P(B_l),$$  

(2.39)

yielding Eqs. (2.30,2.31) directly. This alternative derivation provides a very clear interpretation of our previous result, to those familiar with the data processing inequality. Trying to gather information about $B$ (instead of the maximally refined redundantly imprinted $A$) with the indirect measurement $Y$ (instead of the optimal $X$) can be viewed as the addition of noise over the perfect communication channel that allows the transmission of information about $A$ in the environment.

Equations (2.37-2.38) extend Theorem 2.5.1 to imperfect redundant imprints (i.e. finite $\delta$). Only observables “close” to the maximally refined redundant observable $A$ — where closeness is measured with the help of mutual information $I(B : A)$ — can leave a redundant (even imperfect) imprint in their environment.

**Imperfect correlations**

The previous section analyzed the consequences of perfect correlations between $S$ and $\mathcal{F}$ in terms of optimal measurement strategies. However, perfect correlations are rarely found in Nature. Even for our simple model, perfect correlations arise only in an asymptotic fashion, as $N$ tends toward infinity, or by a careful tuning of the interaction time and strength between $S$ and $\mathcal{E}$. Hence, it is important to understand what happens when the conditions are not ideal. Here, we show that nearly perfect correlations — $\gamma^{\mathcal{F}}$
and $\gamma^F$ sufficiently small — are enough to ensure the validity of the results established above, up to small correction terms.

The technique we use is inspired by perturbation theory. It relies on the construction of a “perfectly correlated” state $\varrho^{SF}$ of the form Eq. (2.27) which is “close” to the actual state $\rho^{SF}$ of Eq. (2.24) generated by the dynamics. Then, using various bounds on entropies, we will conclude that all the information-theoretic quantities extracted from the ideal $\varrho^{SF}$ are approximately equal to those extracted from the actual $\rho^{SF}$. We will also examine the regime of validity of this approximation.

Let us define

$$\varrho^{SF} = \sum_i |\alpha_i|^2 |i\rangle \langle i| \otimes |\Psi^F_i\rangle \langle \Psi^F_i|,$$

where the $|\Psi^F_i\rangle$’s are obtained by applying the Gram-Schmidt orthonormalisation procedure to the states $|\Phi^F_i\rangle$’s (see Appendix A for the details of this construction). With this definition, we will show that for any two observables $B$ and $Y$, when $\gamma^F = \max_{ij} |\gamma^F_{ij}|$ and $\gamma^F = \max_{ij} |\gamma^F_{ij}|$ are small,

$$I_\rho(B : Y) \approx I_\varrho(B : Y).$$

(A2.41)

Above, the subscripts $\rho$ and $\varrho$ refer to the state, either $\rho^{SF}$ or $\varrho^{SF}$, used to derive the probabilities of the measurement outcomes, that in turn are used to quantify information (this shorthand notation will be used in the rest of this section). Therefore, when Eq. (2.41) holds, all the conclusions derived from the perfect correlation case remain approximately true.

Equation (2.41) is a consequence of simple inequalities that give an upper bound on the difference $|I_\rho(B : Y) - I_\varrho(B, Y)|$. First, Cauchy-Schwartz inequality (Proposition A.0.1) gives

$$\text{Tr} |\rho^{SF} - \varrho^{SF}| \leq \sqrt{d^S} \|\rho^{SF} - \varrho^{SF}\|_2$$

where $d^S$ is the dimension of the system of interest. Second, by definition of the trace distance between two density matrices (Definition A.0.1),

$$\sum_{ij} |p_\rho(B_i, Y_j) - p_\varrho(B_i, Y_j)| \leq \text{Tr} |\rho^{SF} - \varrho^{SF}|.$$

Finally, by combining these results with Lemma A.0.1 and Fanne’s inequality (Proposition A.0.3) applied separately to each of the three entropies involved in $I(B, Y) = H(B) + H(Y) - H(B, Y)$, we find

$$|I_\rho(B : Y) - I_\varrho(B : Y)| \leq -3f(\gamma^F, \gamma^F) \log(f(\gamma^F, \gamma^F)/d^S) + O((\gamma^F)^3/4 + (\gamma^F)^2),$$

with $f(\gamma^F, \gamma^F) = \sqrt{d^S (d^S - 1)(\gamma^F)^2 + (\gamma^F)^2}$. Thus, this difference tends to zero when $\gamma^F$ and $(\gamma^F)^{1/2}$ tend to zero.
To gain further insight into the regime of validity of Eq. (2.41), recall that $\gamma_F$ and $\gamma_\bar{F}$ typically decrease exponentially with the number of environmental subsystems that have effectively interacted with $S$. Therefore, for equation Eq. (2.41) to hold within constant accuracy, it is sufficient that each fragment $F$ and $\bar{F}$ contains a number of subsystems $E_k$ scaling as $\log d^S$ (or as a polynomial in $\log d^S$). As discussed at the end of Section 2.3, $d^S$ is the effective dimension of the probed degree of freedom of $S$, i.e. the number of distinguishable outcomes of an hypothetical measurement $B$. Clearly then, $\log d^S$ is generally much smaller than the size of the environment $N$. Therefore, the conclusions drawn from the perfect correlation study remain essentially unchanged: $A$ is the observable of the system that leaves the strongest imprint in fragments of the environment; the optimal environmental measurement to learn about any system observable is the one that reveals information about $A$; and finally failing to interrogate $F$ about $A$ has the same effect as introducing noise in the measurement results. These conclusions hold to within an accuracy of roughly $\log d^S/N$, which is enough in most situations involving typical environments, e.g. photon bath.

**Quantum Darwinism exemplified**

Let us now illustrate the results we have established using the simplest nontrivial instance of our model: the system $S$ and each environmental subsystem $E^k$ are spin-$\frac{1}{2}$ particles. Then, the operators entering in the coupling Hamiltonian Eq. (2.19) can be chosen as Pauli matrices without loss of generality, $A = \sigma^S_z$ and $Z^{E^k} = \sigma^{E^k}_y$, so

$$H^{S,E} = \sum_{k=1}^{N} g_k \sigma^S_z \otimes \sigma^{E^k}_y.$$  \hspace{1cm} (2.42)

We set the initial state of $S-E$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle^{E^1} \otimes \ldots \otimes |0\rangle^{E^N}$ — where by definition $\sigma_z|0\rangle = |0\rangle$ and $\sigma_z|1\rangle = -|1\rangle$ — and let them interact for a time $t$.

The first question to ask is what are the system observables $B$ that can be deduced from measurements on the entire environment; a question that must be addressed before the redundancy of these environmental imprints is studied. As a consequence of basis ambiguity described in Section 2.1, information about many observables $B$ can be deduced by an appropriate measurement on the entire environment. Therefore, completeness of information $\hat{I}_E(B) \approx H(B)$, while a prerequisite for objectivity, is not a very selective criterion.
Figure 2.2: Quantum Darwinism exemplified. All plots are function of the angle $\mu$ between the system observable $B$ and the pointer observable $A = \sigma^S_z$, and the interaction action $a_k = g_k t$ which is defined as the product of the strength and time of interaction.

a) Information retrievable from the entire environment about $B$. b) Redundancy: the number of disjoint fragments of $E$ containing 90% of the information present in the entire environment about $B$. c) Information acquired about $B$ by random measurements performed on individual subsystems of the environment as a function of the size $m$ of the interrogated fragment of the environment.

This is illustrated on Fig. 2.2 a) where we have plotted the information acquired about $B$ by the optimal measurement on the whole environment, $\hat{I}_E(B)$, as a function of the inferred observable $B(\mu)$ and the action $a_k = g_k t = a$ for all $k$. The set of system observables $B$ are parametrized by a single number $\mu$, $B(\mu) = \cos(\mu)\sigma^S_z + \sin(\mu)\sigma^S_x$, where $\mu$ is the angle between $B$ and the pointer observable $A = \sigma^S_z$. The interaction action $a_k = g_k t$ — or more precisely $\sin(a_k)$ — characterizes the strengths of the correlations between $S$ and $E_k$. We see on Fig. 2.2 a) that a large amount of information is accessible in the whole environment for any observables $B(\mu)$ except when the interaction action $a_k$ is pathologically small, i.e. when the interaction time is very short compared to the coupling strength $t \ll 1/g_k$.

We can also evaluate the redundancy of each system observable $B$ by numerically evaluating $\hat{I}_F(B)$ while letting the size of $F$ grow until we find $\hat{I}_F(B) \geq (1 - \delta)\hat{I}_E(B)$ (we have arbitrarily chosen $\delta = 0.1$). Thus, $R_{0.1}(B)$ counts the number of times 90% of the total information can be “read off” independently by measuring distinct fragments of the environment. Note that due to the symmetries of the model, all fragments of $E$ of the same size contain the same information about $S$; this greatly simplifies our...
calculations and the presentation of our results. The results are shown on Fig. 2.2 b). For all values of the action $a_k = g_k t = a$, redundant imprinting is sharply peaked around the pointer observable. Redundancy is a very selective criterion.

According to our general findings of the previous subsections, only observables “close” to $A$ — i.e. $I(B : A) \geq (1 - \delta)\hat{I}_E(B)$ — can leave a redundant imprint on $E$. By carefully tracking all orders of $\delta$, one can show that the existence of a complete and redundant imprint of observable $B(\mu)$ in the environment requires $H_2(\cos^2 \frac{\mu}{2}) \leq \delta$, where $H_2(p) = -[p \log p + (1-p) \log(1-p)]$. Inserting the actual values of the parameters chosen for our simulation, the above equation indicates that only observables with $|\mu| < 0.23$ leave a redundant imprint on the environment: the objective properties of the system are unique. This bound, indicated by a dashed line on Fig. 2.2 b) is in excellent agreement with our numerical results. Surprisingly, and as confirmed by our simulation, the interaction action $a_k$ only plays a role in setting the value of the redundancy at its maximum, but does not affect the selectivity of our criterion. Which observable becomes objective is largely decided by the structure of the interaction Hamiltonian, (i.e. the set of pointer states), but not by its details such as strength and duration of the interaction. This ensures the stability of the pointer observable deduced from redundancy.

The last thing we wish to study with the help of this simple example is an issue that we have not addressed formally in the previous sections. In classical coding theory, redundancy is the simplest form of protection against errors, known as the repetition code. Obviously, losing a few bits or introducing a small number of “bit flips” can be corrected by a suitable majority vote when several copies of the information are present. Robustness of redundantly imprinted information is also crucial for the emergence of an objective reality from environment as a witness. In this context, the most common form of error is the loss of environmental subsystems: a typical observer has access to only a small fragment of the total environment, the rest of $E$ escapes his monitoring. Thanks to redundancy, reliable information about the system preferred observable $A$ can still be deduced from such small fragments of $E$.

Another form of error follows from the observer carrying sub-optimal measurements on his fragment of $E$. Remember that we have so far mainly been interested by optimal measurements of the environment to learn about the system, hence the “hat” on $\hat{I}_E(B)$. However, objective information must be extractable through “realizable”—hence, not necessarily optimal—measurments for many observers to arrive at an operational con-
sensus about the state of a system. For instance, human eyes can only measure photons separately, yet we can still learn about the position of objects. This issue is considered for our model in Fig. 2.2 c), where we have plotted the information about \( B(\mu) \) extracted by an observer restricted to local random measurements on \( m \) environmental subsystems, i.e. \( X = X^{\mathcal{E}_1} \otimes \ldots \otimes X^{\mathcal{E}_m} \) where each \( X^{\mathcal{E}_k} \) is chosen at random. The interaction action \( a_k = g_k t \) is randomly chosen in \([0, \pi/4]\) for each \( k \). As we see, even local (i.e. spin by spin) random measurements eventually (i.e. after measuring roughly 10 spins) acquire the entire information available in \( \mathcal{E} \) about the pointer states.

Though surprising, this result naturally follows from quantum Darwinism and the fact that high redundancy protects information against a wide range of errors. Almost any observable of \( S \) is completely imprinted on the environment (see Fig. 2.2 a)). However, as our general study establishes and Fig. 2.2 b) illustrates, only the observables which are “close” to the maximally refined pointer observable \( A = \sigma_z^S \), can be imprinted redundantly in the environment. Information about any other observable \( B(\mu) \) is restricted by Eq. (2.36) to be equal to the information brought about it by the direct measurement of the pointer observable. Therefore only information about pointer states can tolerate errors, i.e. can be extracted by non-optimal measurements. In short, not only is the information about the pointer observable easy to extract from fragments of the environment, it is impossible to ignore!

We have not proven this fact in the most general setting, but conjecture that it is true: Random measurements carried on fragments of the environments asymptotically yield all the information about the maximally refined redundantly imprinted observable \( A \), provided that redundancy is sufficiently high. For all other system observables, the information acquired in this fashion is bounded by information brought about it by a direct measurement of \( A \) on \( S \).

2.7. Discussion

Environment as a witness view of the origin of our perception of classicality as well as quantum Darwinism — the dynamics responsible for the redundant imprinting of certain states that leads to the emergence of objectivity — are based on the same model of measurements that is used in the study of decoherence and einselection. The to-be-classical “object of interest” (the system \( S \) or the apparatus \( A \)) is immersed in the environment. What is now different — and this is a dramatic departure from the
usual view of what matters — is the focus of attention. Instead of analyzing either the state of $S$ *per se*, or even the fate of the correlations between $S$ and $A$, the focus shifts to the information available to the observer in *fragments* of $E$. By doing so, we have demonstrated, under reasonable assumptions, that independent observers will arrive at a consensus about the properties of the system.

**Assumptions**

The aim of this section is to examine assumptions that went into our discussion and, by doing so, to explore the range of validity of our conclusions. The results obtained in Section *Consequences of redundancy* 2.5 did not require any assumption about the physical model, but only apply to the case of perfect correlations. Thus, the model studied in Section *Quantum Darwinism: dynamical emergence of objectivity* 2.6 is a convenient focus of attention. To establish uniqueness of the preferred observable that is easiest to infer from $E$, we have assumed that:

1. The initial state is a pure product state.
2. The system has no self-Hamiltonian.
3. Every environmental subsystem couples to the same system observable.
4. The environment has no Hamiltonian.

To find out which of these assumptions can be relaxed, and the extent to which they are responsible for the conclusions we have reached will eventually require investigation of other, more realistic, or at least “differently oversimplified” models. For “standard” decoherence, a similarly idealized model was put forward over two decades ago, but the investigation of various related and unrelated models of decoherence and einselection is still an ongoing activity, often yielding new insights. The same can be expected of quantum Darwinism. Different models may also require different mathematical tools. One such investigation has recently been realised [BKZ04a] and points toward compatible conclusions. All we can offer here is therefore a brief (and possibly premature) discussion of the role and importance of various assumptions, including these listed above.

**Assumption 1** is probably the most unrealistic: in practice composite environments are rarely in a pure product state. Luckily, perfect purity *per se* is not essential to rely
on the environment as a trustworthy witness. Having enough information about $\mathcal{E}$ will, however — and in contrast to decoherence and einselection — prove to be indispensable.

Indeed, it is often convenient to study decoherence assuming a very mixed state of the environment (i.e., thermal equilibrium or even a perfect mixture) when deriving master equations used to implement predictability sieve. Consequences of different initial mixtures of $\mathcal{E}$ are, generally, somewhat different time dependences, and minor changes in the structure of the master equation (that often becomes less Markovian and less tractable when the environment is further away from a convincing thermal state), but the key qualitative conclusions that characterize decoherence and einselection — the localized nature of the preferred states and the fact that relaxation can be much slower than decoherence — seem to be usually unaffected.

By contrast, the degree of ignorance about the fragments of the environment plays an essential role in the study of quantum Darwinism. The reader may be surprised by this. After all, the results of Section 2.5 and 2.6 were derived by an information theoretic analysis of a rather general scenario, so — given the assumptions — conclusions should be independent of the initial state of $\mathcal{E}$. In particular, redundancy — when present — remains a highly selective criterion. However, and this is the crux of the matter, the starting point of our investigation — the assumption that fragments of the environment contain some information about the system — depends strongly on the initial state of $\mathcal{E}$.

When the environment is initially mixed, it will “know less” about the system. To see why, let the initial state of the environment be an arbitrary non-entangled state:

$$\rho^E = \sum_{\ell} p_\ell \bigotimes_{\mathcal{E}_k} |\phi^{E_k \ell}\rangle \langle \phi^{E_k \ell}|. \quad (2.43)$$

In particular, it could be a product of mixed states $\rho^E = \rho^{E_1} \otimes \rho^{E_2} \otimes \ldots \rho^{E_N}$, such as the thermal state of non-interacting environmental subsystems. By linearity of the Schrödinger equation, the joint state of $S$ and a fragment $\mathcal{F}$ of $\mathcal{E}$ after an interaction time $t$ will be

$$\rho^{SF} = \sum_{\ell} p_\ell \sum_{ij} \alpha_i \alpha_j^* |i\rangle \langle j| \bigotimes_{\mathcal{E}_k} |\phi^{E_k \ell}_i\rangle \langle \phi^{E_k \ell}_j| \times \gamma_{ij}^{\mathcal{F} \ell} \quad (2.44)$$

where $|\phi^{E_k \ell}_i\rangle$ and $\gamma_{ij}^{\mathcal{F} \ell}$ are defined as in Section 2.6.1.

In Sections 2.6, we have studied the kinds of correlations that arise given any of the components $\bigotimes_{\mathcal{E}_k} |\phi^{E_k \ell}\rangle$ of this mixture. It follows from the convexity of entropy (c.f.
Proposition A.0.4) that the information contained in this mixture will be strictly less than the average information contained in the individual components of the mixture. This can be understood intuitively: mixing up the state of the environmental subsystems decreases their information storage capacity. For instance, when the state of the environment is perfectly mixed, it will simply be impossible to learn anything from it. Yet, the usual decoherence still leads to einselection — there will still be a pointer basis (defined e.g. through the predictability sieve).

When the initial state of $E$ is not totally mixed, it is usually possible to extract from it some information about the system. In fact, given the assumption of redundancy, the qualitative conclusions of the previous section will still hold: the information about any system observable available in fragments of $E$ is intrinsically limited by the information about it obtained through a direct measurement of the maximally refined redundantly imprinted observable $A$; Eq. (2.36) becomes the inequality $\hat{I}_F(B) \leq I(B : A)$. Therefore, we again anticipate the conclusion that only observables “close” to $A$ can get redundantly imprinted in $E$. Exactly how mixed can $E$ be to be still useful is of course the key question. We leave it as a subject for further research.

When the initial state of the system is mixed, but the environment is sufficiently pure and large so that significant redundant imprinting can arise from their interaction, environment can become a useful and trustworthy witness, and the environment as a witness approach should go through essentially unimpeded. Indeed, this complication should not change basic steps of our analysis. Similarly, preexisting correlation with $E$ need not undermine our conclusions. In effect, it will typically mean that the environment was gathering evidence about the system in the past (although one can certainly imagine pathological preexisting correlations that get undone by the subsequent interaction).

To sum up, while the assumption of the initial product state has simplified our analysis, it can be easily relaxed without undermining our basic conclusions. What is non-negotiable is the demand for the final state that allows one to discern evidence about $S$ in the fragments of $E$. One can already anticipate that this demand will also put a constraint on the entanglement between the fragments of $E$, as we shall note in the discussion of assumption 4 below.

Assumption 2 precludes non-trivial evolution of the system. Relaxing it has been studied in the context of decoherence and einselection, and — as we have done above — we shall gain insight into its role in quantum Darwinism by recounting the implications of
evolution for einselection, and analyzing what they imply for the role of the environment as a witness.

In the studies of einselection the relative strength of the self-Hamiltonian $H^S$ and the interaction Hamiltonian $H_{SE}$ is an important ingredient that decides the course and effect of einselection. When the self-Hamiltonian is negligible or when $H^S$ and $H^{SE}$ commute, the environment monitors static states of the system — pointer states selected solely by the interaction [Zur81a, Zur82a]. In a sense, the environment contains a record of a very uneventful history — things stay the same forever. One may enter, for example, the “Zeno regime” where the evolution of the state of the system induced by the self-Hamiltonian is impeded by the environmental monitoring mediated by $H^{SE}$ (see, e.g., [GJK+96a]). Tractable models of such situations have been analyzed using rather different approach of quantum trajectories [Car93a, DDZ01a].

As the coupling to the environment becomes weak the problem may become tractable again, especially in two rather different limits. When the environment is slow, with the high-frequency cutoff small compared to the level spacing of the spectrum of $H^S$, einselection enters its quantum limit [PZ99b]. Energy eigenstates are imprinted on the environment more or less regardless of the specific form of the coupling. Histories are again becoming rather uneventful, although for reasons quite different from these we have mentioned above in the negligible $H^S$ case.

By contrast, when the environment is “broadband”, with all the frequencies from very low to very high present, and the system is (at least approximately) linear and coupled to $E$ through its position, coherent states are the most predictable, and hence, pointer. Weak coupling need not preclude redundancy of the records. In this underdamped limit one can recover approximately reversible Liouvillian dynamics with localized states (i.e., approximately reversible classical trajectories that follow Newton’s laws emerge; see e.g. [PZ01a, Zur03a], and references therein). When the system is linear (e.g., harmonic oscillator) the preferred pointer states turn out to be Gaussian ([Zur93b, ZHP93a]), and one may anticipate that sequences of the most redundant “environmental records” will correlate with classical trajectories.

The quick summary of different possibilities above is meant to be suggestive rather than exhaustive, and is definitely not conclusive. What one would like to recover using environment as a witness is the notion of objective histories defined through sequences of time-ordered redundant records. Such objective histories could consist of
sequences of approximate instantaneous pointer states. They were conjectured to exist in the limit of very efficient and frequent broad-band monitoring by the environment in [Zur03a]. Histories deduced from redundant records would be objective, and may be only approximate. It will be interesting to investigate their relation to consistent histories [Gri84a, GH90a, Omn92a, GO99a], especially when their consistency is assured through the “strong decoherence” condition introduced in [GH97b] (see also [Hal99b]) that invokes existence of a perfect environmental record.

**Assumption 3** assures that there is a preferred observable of $S$ that is recorded by $E$, and that it is singled out by the interaction Hamiltonian. This is a very strong assumption, but also a reasonably realistic one, so we shall not apologize for it too much. In particular, typical couplings between the systems (and, hence, between $S$ and $E$) often depend on the distance between them. As a consequence — as was pointed out in the context of einselection [Zur82a, Zur91a] — pointer states are localized in position.

One can of course imagine situations where this is not the case. For instance, there may be several physically distinct environments, each attempting to monitor a different observable of $S$. One would expect that a dominant coupling would then impose its selection of the preferred observable, and the effect of the others would be perceived as noise.

**Assumption 4** assures that the environment does not evolve (and, therefore, does not complicate or even obliterate the record it has made of $S$). One can distinguish three components of this requirement: fragments of the environment could evolve separately, they could interact with each other, or could interact with more distant “second order” environments. Let us first note that self-Hamiltonians of the individual fragments of $E$ can be absorbed by the redefinition of the local algebra of observables. Thus, providing that they do not impede redundant imprinting of the preferred properties of the systems in the first place, they can be essentially ignored in our analysis.

By contrast, the interaction between the subsystems of $E$ may be a significant complication. It will typically lead to entanglement between the fragments of $E$, and could make their individual states mixed. Thus, — as we have already pointed out in discussion of assumption 1 — even though the environment as a whole may still contain redundant imprint of the state of the system, the relevant global observables could become effectively inaccessible to the observers who can sample $E$ only through local measurements on its fragments.
The state $\rho^{SE}$

We have argued in Chapter 1 that the state of a quantum system reflects the subjective knowledge of an observer: this is in fact what motivated us to look for a mechanism through which the objective properties of the classical world could emerge. However, one of the central mathematical ingredient to the entire present Chapter is the joint state $\rho^{SE}$ of the system and the environment. It is this state that allows us to assign probabilities to various hypothetical measurement outcomes, and arrive at the conclusion that the set of possible correlations between the system and fragments of the environment implies selection of a preferred observable. The obvious question that comes up then is “Whose Knowledge” [Mer01b] is described by the state $\rho^{SE}$?

In fact, $\rho^{SE}$ does not represent anyone’s knowledge; its sole purpose is to make sure that the restrictions on the correlations between various subsystems imposed by quantum
The simplest way to explain this is through an example.

Suppose that two independent observers, say Gilles and Ray, are monitoring the environment of a system $S$ in order to learn about it. For simplicity, we will suppose that there are only two environmental subsystems, $E_1$ and $E_2$ accessible respectively to Gilles and Ray, and that the system $S$ and both environmental subsystems are spin-$\frac{1}{2}$ particles. Just like in the example at the end of Section 2.6, the coupling Hamiltonian is given by Eq. (2.42). According to their beliefs, Gilles and Ray initially assign to $S - E$ the respective state

$$
\rho^{SE}_G(0) = |+^S_x\rangle \otimes |0^{E_1}\rangle \otimes |+^{E_2}_y\rangle \\
\rho^{SE}_R(0) = |+^S_x\rangle \otimes |+^{E_1}_y\rangle \otimes |0^{E_2}\rangle,
$$

where $\sigma_{x,y}|\pm x,y\rangle = \pm |\pm x,y\rangle$. There is nothing wrong with these states being different of course since they represent their respective knowledge, which can be different. Now, the two environmental subsystems interact with the system for a time $t = \pi/4g$, where the coupling strength of Eq. (2.42) are assumed to be equal $g_1 = g_2 = g$. It is quite simple to show that the two states of Eq. (2.45) will have evolve at time $t$ into

$$
\rho^{SE}_G(t) = \frac{1}{\sqrt{2}} \left( |0^S\rangle \otimes |+^{E_1}_x\rangle \otimes |+^{E_2}_y\rangle + |1^S\rangle \otimes |+^{E_1}_x\rangle \otimes |+^{E_2}_y\rangle \right)
$$

and

$$
\rho^{SE}_R(t) = \frac{1}{\sqrt{2}} \left( |0^S\rangle \otimes |+^{E_1}_x\rangle \otimes |+^{E_2}_x\rangle + |1^S\rangle \otimes |+^{E_1}_x\rangle \otimes |+^{E_2}_x\rangle \right);
$$

according to Gilles, $S$ and $E_1$ are in a maximally entangled state, while according to Ray, it is $S$ and $E_2$ that are in a maximally entangled state. Thus, both Gilles and Ray are in a position where they believe they can use their fragment of $E$ to predict the outcome of any measurement on the system. There is redundant spreading of information without selection of a preferred system observable!

The solution to this puzzle of course is that it is impossible for both $S - E_1$ and $S - E_2$ to be in a maximally entangled state: entanglement is monogamous [TWD03a]. Thus, the states assigned by the two observers are incompatible with each other. Consequently, they can arrive at predictions about the system that contradict each other. For example, Gilles could measure the observable $\sigma_{x}^{E_1}$ on his chunk of $E$ and obtain the outcome “+”,

theory are satisfied.
while Ray could measure \( \sigma_z^E \) on his chunk of \( E \) and obtain the result “−”. This pair of outcome is possible from both Gilles and Ray’s point of view: they both assign a probability 1/4 to it. But then, the state assigned to \( S \) by Gilles would be \( |0^S\rangle \) while the one assigned by Ray would be \( |1^S\rangle \). In this case, a direct measurement of \( \sigma_z^S \) on \( S \) could discriminate between the two predictions.²

Hence, the role of the state \( \rho^{SE} \) is to make sure that the various states assigned by different observers — or more precisely their various knowledge — are compatible [BFM02a, CFS02c, PBK03a] with each other. One can think of \( \rho^{SE} \) as the state that an imaginary “super-observer”, who has access to the information of all other observers, would assign to the system and environment. If the prior knowledge of the observers are in direct contradiction, then the super-observer will not be able to assign any state \( \rho^{SE} \), he will conclude that some of this information has to be wrong. In this case, we cannot guarantee the emergence of a consensus among the various observers, but this should not be surprising. In fact, the same problem can arise classically.

The whole situation can be summarized by “state of knowledge versus state of belief”. In the Bayesian approach to classical probabilities, there is always a choice prior probability assignment \( P(X) \). This prior reflects the observer’s initial subjective belief about the value of \( X \). Bayes rule prescribes how to update the state given some newly acquired data \( D \), but the choice of prior is arbitrary. The state \( P(X|D) \) thus reflects the observed data \( D \), but also generally contains some relics of the initial arbitrary and subjective belief of the observer. In particular, if the observer initially believed some particular value \( X_0 \) of \( X \) to be impossible, i.e. \( P(X_0) = 0 \), then no observation will ever convince him otherwise. Indeed, whatever \( D \) is, \( P(X_0|D) = P(D|X_0)P(X_0)/P(D) \) always equals 0. Hence, if the prior of two observers have disjoint support, then this will always be the case, so they will never reach an agreement.

Moreover, this arbitrary prior assignment is unavoidable, the state cannot be based solely on observed data. This is because a measurement apparatus in a random state cannot be used to extract information. To learn new data, the observer must know something about the measurement apparatus; this knowledge must either come from a previous observation, using an other measurement apparatus, or must simply be as-

²This example is “extreme” in the sense that it lead the two observers to assign orthogonal states to the system. In some other cases, no “single shot” experience will be able to determine what went wrong with this state assignment.
sumed; there is no free lunch, no information without information. What is interesting is to see that when the arbitrary subjective prior states of independent observers are compatible with each other, then a consensus can emerge. Hence, the role of $\rho^{SE}$ is simply to enforce the constraints imposed by quantum theory on the possible relations between subsystems, under the assumption of compatible initial state assignment between the various observers. Just like in the classical setting, the emergence of a consensus cannot be guaranteed when the priors are incompatible.

2.8. Summary and Conclusion

Quantum Darwinism uses the same model of the information transfer that was introduced to study decoherence and einselection, but asks a different question: instead of focusing — as does decoherence — on how the information is lost from the system, it analyzes how the information is gained and stored in the environment. In decoherence, the role of environment is limited to hiding the underlying quantumness (view especially emphasized in discussions of quantum computation). Einselection recognizes that this information loss is sometimes selective, and, thus, that the environment has a capacity to single out preferred pointer states that are best at surviving immersion in $E$. Moreover, they are chosen in the process reminiscent of a measurement — $E$ acts as an apparatus that (pre-)measures the pointer observable of the system of interest.

This much was known. In particular, the monitoring role of $E$ was recognized early on [Zur81a]. Quantum Darwinism proposes the answer to the next logical question: since the environment interacts with the to-be-classical observable of the system of interest as would an apparatus, can it be used as an apparatus? To address it we have had to develop a measure of the objectivity of the records deposited in the environment. Redundancy was used to prove that — given reasonable assumptions — there is a unique observable that is easiest to find out from fragments of $E$, and that this most redundantly recorded observable coincides with the familiar pointer observable.

As a consequence, observers monitoring a fragment of the environment will become correlated with the system’s pointer observable. Each of them will then be able to reach identical conclusions about the value of the redundantly imprinted observable of the system, i.e. about the objective properties of the system. In this operational sense, quantum Darwinism provides a satisfying explanation for the emergence of the objective classical world we perceive from the underlying quantum substrate.
We have illustrated quantum Darwinism on a dynamical model that is easy to analyze in the information theoretic terms and, yet, is inspired by a photon environment scattering on an object: all the environmental subsystems couple to the object with the same Hamiltonian and do not interact with each other. This model enabled us to push our analysis further, as we could explicitly determine the optimal environmental measurements to learn about the properties of the system. It also demonstrated that quantum Darwinism tolerates reasonable departures from the “ideal” assumptions used to derive our main results in Section 2.5. In this respect, it corroborates our conjecture (see also [Zur03a]) that noted the role of redundancy in assuring resilience of certain states — an essential feature of the classical domain. Hence, redundancy is a robust and selective criterion for determining objective properties of open quantum systems.

While redundantly imprinted observables are dynamically stable — as defined by einselection — the reverse is not necessarily true: quantum Darwinism requires stronger assumptions, especially regarding structure, size, and the initial state of $E$. For example, a single photon can be enough to decohere an object in superposition of two distinct positions. However, it takes a macroscopic number of them to redundantly broadcast the position of this object throughout the environment. While the entropy production of the system — a signature of decoherence — rapidly saturates, redundancy can then continue to grow with time. This illustrates how the increase of the redundancy of the record in the environment captures the significance of the fact that the system is still continuously “under observation”, and that information about the pointer observable is getting amplified up to the macroscopic level. In this sense, one might regard quantum Darwinism as a fully quantum implementation of Bohr’s idea [Boh58a] about the role of amplification in the transition from quantum to classical.
Summary of Chapter 2

- Independent observers performing arbitrary direct measurements on a quantum systems will not reach a consensus about their findings.

- When a system is immersed in an environment, it is possible to learn about it indirectly by measuring $\mathcal{E}$. Even through such indirect measurement, independent observers can generally not reach a consensus about the properties of the system, a symptom of the basis ambiguity.

- For many observers to independently arrive at consensus about the properties of $\mathcal{S}$ through indirect measurements, the environmental imprint must be redundant.

- Redundant proliferation of information about $\mathcal{S}$ in $\mathcal{E}$ implies selection of a preferred system observable $A$: only the system observables $B$ “close” to $A$ can leave a redundant record in $\mathcal{E}$, and thus can be discovered indirectly.

- Measurements performed on fragments of $\mathcal{E}$ can at best be used to simulate a direct measurement of $A$ on $\mathcal{S}$: hence, they behave as if the system had an objective state, one of eigenstates of $A$.

- Redundancy implies robustness of the information recorded in $\mathcal{E}$: Information learned indirectly about $\mathcal{S}$ appears to be insensitive to changes in strategy through which $\mathcal{E}$ is interrogated as well as strength and duration of the interaction between $\mathcal{S}$ and $\mathcal{E}$. 
3 — Macroscopic observables

[...] we learn from quantum theory that the appropriateness of our usual causal space-time description depends entirely upon the small value of the quantum of action as compared to the actions involved in ordinary sense perceptions. [Boh28a]

— Niels Bohr

3.1. Overview

The aim of the present Chapter is to demonstrate that “classical reality” can emerge through macroscopic observables, that arise when a collection of quantum systems are measured jointly. Since the physical scale of individual quanta is generally tiny, macroscopic observables are typically the only observables that are directly accessible to our senses. Formally, they can be described by type projectors, which reveal information about the average population of single-particle states. For example, the total magnetization of an ensemble of spin-$\frac{1}{2}$ particles provides some information about the relative occupation number of the spin up and spin down states. We will derive several general properties of these measurement and discuss how they lead to the emergence of a quasiclassical domain in the absence of large scale entanglement.

The effect of macroscopic observations on infinite ensemble of identically prepared quantum systems has been studied in various contexts [Fin63a, Har68a, Gra73a, FGG89a]. The main conclusion of these studies is that the state $|\psi\rangle^\otimes N$ describing such an ensemble is an eigenstate of type projectors when $N = \infty$. However, for finite ensembles, things change dramatically. The measurement of a macroscopic observable induces a disturbance which increases as the size of the ensemble grows, in apparent contradiction

1 Of course, indirect measurements, as those discussed in the previous Chapter, can reveal information about the microscopic properties of the world.
with the infinite-copy result. This discrepancy follows from the ambiguous extension of finite-copy considerations to the nonseparable Hilbert space of an infinite-copy ensemble [CS04a]. One of the core mathematical achievements of the present Chapter is to show how the essence of the infinite-copy result can be recovered for finite ensembles by “smoothing” the type projectors into coarse-grained positive operator valued measurement (POVM) (essentially going from the strong to the weak law of large numbers).

The Chapter is organized as follows. The central mathematical objects are defined in Section 3.2. We first summarize the method of type and define type projectors. These are projectors on the degenerate eigensubspaces of macroscopic observables of the form $A_N = \sum_{k=1}^{N} a_{(k)}$, where $a_{(k)}$ is a physical observable acting on the $k$th system of the ensemble. Using the theory of generalized measurements, we also define coarse-grained POVMs corresponding to finite accuracy estimation of a macroscopic observable.

Section 3.3 contains the core mathematical analysis of our study. We first recapitulate the well known facts about type projectors acting on infinite ensembles and show how they dramatically break down for finite ensembles. Then, we show how the result is approximately recovered when the measurements are of finite accuracy, and study the general tradeoff between measurement coarseness and state disturbance — measured in terms of fidelity — as a function of the size of the ensemble. In short, we demonstrate that a measurement of coarseness $\sigma \gg 1/\sqrt{N}$ leaves the systems essentially unchanged, i.e. the fidelity $F$ between the pre- and post-measurement state of the ensemble satisfies $1 - F \propto \frac{\ln(N\sigma^2)}{N\sigma^2}$.

Section 3.4 is a discussion of the de Finetti representation theorem which is of prime importance to bridge the gap between subjective quantum states and the objective physical reality. The exchangeable states described by this Theorem have recently been employed for the discussion of quantum state tomography based on single-system measurements followed by Bayesian update [CFS02b]. We will show how macroscopic observables offer an alternative perspective on quantum tomography. Moreover, this approach offers interesting applications for quantum information theory [HM02a, BHL04a] and is a more accurate description of experimental spectroscopy-based implementations of tomography, e.g. as achieved in Ref. [VFP+01a].

Most importantly, macroscopic observables also provide an explanation for the emergence of the classical world we perceive from the underlying quantum theory. Indeed, we demonstrate in section 3.5 that in the absence of large-scale entanglement, one of the
main characteristics of the classical domain follows naturally from the general properties of coarse grained type POVMs: they behave as if they were revealing information about an underlying objective reality. This is done using the consistent histories formalism which we briefly summarize. We demonstrate that the histories generated by any sequence of macroscopic observables of accuracy $\sigma \gg \sqrt{\xi/N}$ are consistent, where $\xi$ is the quantum correlation length-scale of the system. This generalizes some ideas introduced by Halliwell [Hall98a, Hall99a] on how to achieve classicality in closed quantum systems.

Finally, Section 3.6 discusses the role of macroscopic observables in NMR quantum information processing. In this context, macroscopic observables are used to extract the output of the computation, but also, since the measurement device can not be “turned off” — i.e. the state of the processor can always be read-off from the spectrometer — they constantly perturb the computation. Following the results of Section 3.3 and a measurement model introduced in Ref. [LS00b], we show that the measurements used in NMR can in principle be sufficiently precise to extract useful information about the computation but yet so coarse grained that they induce a negligible perturbation. However, as we will demonstrate, NMR measurements may not follow our optimal measurement coarseness-state disturbance tradeoff when performed at room temperature; caution is advised when applying our conclusions. Finally, Section 3.7 summarizes our results and discusses some open questions.

3.2. Definitions

This section contains all the mathematical definitions required for the present Chapter. Our general setting consists of an ensemble of $N$ quantum systems of the same nature. For sake of clarity, we adopt the vocabulary of NMR. Therefore, we shall refer to individual systems of an ensemble as molecules and to the ensemble of $N$ molecules itself as the sample. Thus, the word “molecule” should not be taken literally in what follows; it could be any elementary constituent of a larger system.

*Method of types*

The method of type is a very powerful statistical tool with applications ranging from large deviation theory, universal coding, and hypothesis testing. We will only scratch the surface of this theory here, more details and applications can be found in [CT91a]
Macroscopic observables

Let \( X = x_{j_1} x_{j_2} \ldots x_{j_N} \in \mathcal{X}^N \) be a string of \( N \) letters drawn from a \( d \)-letter alphabet \( \mathcal{X} = \{ x_1, x_2, \ldots, x_d \} \). The type (or empirical probability distribution) of \( X \) is a vector of positive numbers summing to one defined by

\[
\mathbf{L}(X) = \left( L_1(X), L_2(X), \ldots, L_d(X) \right),
\]

where \( L_j(X) \) is the relative frequency of the letter \( x_j \) in the string \( X \)

\[
L_j(X) = \frac{1}{N} \sum_{k=1}^{N} \delta_{j,k};
\]

it is simply the number of occurrences of the letter \( x_j \) in \( X \), divided by the length of \( X \). For example, if \( \mathcal{X} = \{a, b, c\} \) and \( N = 4 \), then \( \mathbf{L}(cbaa) = (\frac{1}{2}, \frac{1}{4}, \frac{1}{4}) \). We also define a type class \( T \) to be the set of strings of a given type:

\[
T[\mathbf{L}] = \{ X \in \mathcal{X}^N : \mathbf{L}(X) = \mathbf{L} \}.
\]

For example, using the same alphabet as above, we have \( T[(\frac{1}{4}, 0, \frac{3}{4})] = \{ accc, cacc, ccac, ccca \} \). The class \( T[\mathbf{L}] \) can be generated by applying all permutations to any single string of type \( \mathbf{L} \). Hence, the number of elements in \( T[\mathbf{L}] \) is given by the multinomial coefficient

\[
|T[\mathbf{L}]| = \binom{N}{NL_1, NL_2, \ldots, NL_d} = \frac{N!}{(NL_1)!(NL_2)! \cdots (NL_d)!}.
\]

Let \( \mathbf{R} = (R_1, R_2, \ldots, R_d) \) be a probability distribution over \( \mathcal{X} \). The probability of the string of outputs \( X = x_{j_1} x_{j_2} \ldots x_{j_N} \) of \( N \) letters, each drawn independently according to the distribution \( \mathbf{R} \), is \( P(X) = R_{j_1} R_{j_2} \ldots R_{j_N} \). This can also be written as

\[
P(X) = R_1^{NL_1(X)} R_2^{NL_2(X)} \ldots R_d^{NL_d(X)},
\]

so given a fixed distribution \( \mathbf{R} \), the probability of a string \( X \in \mathcal{X}^N \) depends only on its type. Intuitively, the type of the observed outcome \( X \) is very likely to be close to the probability distribution of the random variable, i.e. \( L_j(X) \approx R_j \), as \( N \) increases. This is the substance of the typical sequence theorem [CT91a]:

\[
P(\| \mathbf{L} - \mathbf{R} \|^2_1 > \epsilon) \leq e^{-N(\epsilon/2 - d \ln(N+1) / N)} \approx e^{-N\epsilon/2}
\]

where the “difference” between the type \( \mathbf{L} \) and the probability distribution \( \mathbf{R} \) is quantified by the variational distance (\( L_1 \)-norm)

\[
\| \mathbf{L} - \mathbf{R} \|_1 = \sum_j |L_j(X) - R_j|.
\]
The typical sequence theorem takes on various forms. It can be formulated in a stronger version using the relative entropy, which is an upper bound to the variational distance. Nevertheless, for our considerations, this simple version will be sufficient.

**Macroscopic observable**

Using this notation, we now formally define macroscopic observables. Consider a Hermitian operator (i.e. *observable*) \( a \) acting on the \( d \)-dimensional Hilbert space of a single molecule \( \mathcal{H}_m \). Let \( \{|x_1\rangle, |x_2\rangle, \ldots |x_d\rangle \} \) and \( \{\alpha_1, \alpha_2, \ldots, \alpha_d\} \) denote its eigenvectors and eigenvalues: \( a|x_j\rangle = \alpha_j|x_j\rangle \). We will assume that \( a \) is *non-degenerate*, generalization is straightforward. The macroscopic observable \( A_N \) corresponds to the sum of observable \( a \) over all the \( N \) molecules of the sample,

\[
A_N = \sum_{k=1}^{N} a(k),
\]

where \( a(k) \) is the operator \( a \) acting on the \( k \)th molecule,

\[
a(k) = \underbrace{1 \otimes \cdots \otimes 1 \otimes a \otimes 1 \otimes \cdots \otimes 1}_{N-k}.
\]

The operator \( A_N \) acts on the joint Hilbert space of the \( N \) molecules \( \mathcal{H}_s = \mathcal{H}_m^\otimes N \) — the Hilbert space of the sample — which has dimension \( d^N \). We use the standard abbreviation \( |X\rangle = |x_{j_1}\rangle \otimes |x_{j_2}\rangle \otimes \ldots \otimes |x_{j_N}\rangle \) for each string \( X \in \mathcal{X}^N \). Clearly, the states \( \{|X\rangle\} \) form an orthonormal basis for \( \mathcal{H}_s \). Moreover, they are eigenstates of the macroscopic observable \( A_N \):

\[
A_N|X\rangle = A_N|x_{j_1}\rangle \otimes |x_{j_2}\rangle \otimes \ldots \otimes |x_{j_N}\rangle
= \sum_{k=1}^{N} a(k)|x_{j_1}\rangle \otimes |x_{j_2}\rangle \otimes \ldots \otimes |x_{j_N}\rangle
= \sum_{k=1}^{N} \alpha_{j_k}|x_{j_1}\rangle \otimes |x_{j_2}\rangle \otimes \ldots \otimes |x_{j_N}\rangle
= \sum_{k=1}^{N} \alpha_{j_k}|X\rangle = \left( \sum_{j=1}^{d} NL_j(X)\alpha_j \right)|X\rangle.
\]

Thus, we see that the eigenvalue associated to a basis state \( |X\rangle \) depends only on its type \( L(X) \). As a consequence, the degenerate eigensubspaces of \( A_N \) are those subspaces spanned by the vectors \( |X\rangle \) belonging to the same type class.
This brings us to the definition of type measurements which are von Neumann measurements composed of the projection operators on the subspaces of a given type:

\[ Q_L^{(N)} = \sum_{X \in T[L]} |X\rangle \langle X|. \] (3.4)

Each of these type projectors is labeled by a vector of \( d \) positive numbers \( L_j \) which correspond to the type \( L(X) \) of the basis vectors \( |X\rangle \) spanning the subspace. Obviously, the projectors \( Q_L^{(N)} \) depend on the choice of basis \( |x_j\rangle \) over \( \mathcal{H}_m \), i.e. on the eigenvectors of the observable \( a \), so we could explicitly note \( Q_L^{(N,a)} \). Moreover, we would like to stress that the spectral projectors \( Q_L^{(N,a)} \) and \( Q_L^{(N,b)} \) associated to two distinct macroscopic observables \( A_N = \sum_k a(k) \) and \( B_N = \sum_k b(k) \) do not commute, unless the underlying single-molecule observables \( a \) and \( b \) happen to commute. To avoid cumbersome notation however, we will only use an extra superscript when necessary (c.f. Section 3.4.1). For the time being, we will consider a fixed arbitrary macroscopic observable \( A_N \). In this case, it is straightforward to verify that the type projectors are mutually orthogonal and that they sum to the identity

\[ Q_L^{(N)} Q_{L'}^{(N)} = \delta_{L,L'} Q_L^{(N)}, \quad \sum_L Q_L^{(N)} = \mathbb{1}. \] (3.5)

In words, these projectors correspond to the exact measurement of the population of the levels \( |x_j\rangle \) over an ensemble of \( N \) molecules, without distinguishing between the molecules of the sample. The type projectors \( Q_L^{(N)} \) allows us to express the operator \( A_N \) in a simple form:

\[ A_N = \sum_L A_L Q_L^{(N)} \] (3.6)

where we have defined \( A_L = \sum_{j=1}^d NL_j \alpha_j \). This decomposition follows straightforwardly from Eq. (3.3) as all the states \( |X\rangle \) with \( L(X) = L \) composing the projector \( Q_L^{(N)} \) have eigenvalue \( A_L \). Similarly, any macroscopic observable of the form Eq.(3.2) has a spectral decomposition involving only type projectors, as in Eq.(3.6). Hence, following textbook quantum mechanics, when measuring a macroscopic observable — or measuring the “expectation value” of a physical observable over a macroscopic sample —, one is really performing a projective von Neumann measurement composed of type projectors.

These type projectors have been studied under many different forms [Fin63a, Har68a, Gra73a] and take on many different names. Among other formulations are the frequency...
operators. Recall that $L_j(X)$ is the relative frequency of the symbol $x_j$ in the string $X$. We can define a frequency operator

$$F_j^{(N)} = \sum_X L_j(X)|X\rangle\langle X|.$$

This operator is a macroscopic physical observable whose eigenvalues are \(f_j = 0, \frac{1}{N}, \frac{2}{N}, \ldots, 1\). Indeed, \(F_j^{(N)}\) takes on the form of Eq. (3.2) by setting the single-molecule observable \(a\) to \(\frac{1}{N}|x_j\rangle\langle x_j|\). Following textbook quantum mechanics, when the measurement associated to \(F_j^{(N)}\) is performed and eigenvalue \(f_j\) is observed, the state of the system gets collapsed to the subspace spanned by the states \(|X\rangle\) for which \(L_j(X) = f_j\). Hence, the eigenvalue \(f_j\) indicates the relative population of the single-molecule state \(|x_j\rangle\) in the sample of \(N\) molecules.

The above construction yields \(d\) commuting physical observables \(\{F_j^{(N)}\}_{j=1,\ldots,d}\), one for each single-molecule state \(\{|x_j\rangle\}_{j=1,\ldots,d}\). Regrouping these observable into a \(d\)-component observable yields

$$F^{(N)} = (F_1^{(N)}, F_2^{(N)}, \ldots, F_d^{(N)}) = \sum_L LQ_L^{(N)},$$

which takes on the form of Eq. (3.6), with a \(d\)-component eigenvalue \(A_L = L\). The value of any macroscopic observable of the form Eq. (3.6) can be deduced straightforwardly from the value of \(F^{(N)}\). Hence, a great deal of attention has been focused on the macroscopic observable \(F^{(N)}\), without loss of generality.

We illustrate macroscopic observables for a sample of \(N\) spin-$\frac{1}{2}$ particles. We choose the basis \(|x_1\rangle = |\uparrow\rangle\) and \(|x_2\rangle = |\downarrow\rangle\) corresponding, respectively, to +1 and -1 units of magnetization ($\frac{1}{2}\hbar g$) in the \(z\) direction:

$$\sigma^z|x_1\rangle = +|x_1\rangle \text{ and } \sigma^z|x_2\rangle = -|x_2\rangle.$$

We can use a single positive number \(L \in \{0, \frac{1}{N}, \frac{2}{N}, \ldots, 1\}\) to label the type of a binary string \(X\), which corresponds to the fraction of \(x_1\)'s (or spin up's) in \(X\). Hence, a type \(L\) is a shorthand for \(L = (L, 1 - L)\). The bulk (or total) magnetization of the sample is equal to the sum of the magnetization of each molecules: the corresponding operator is therefore $M^z = \sum_k \sigma_k^z$, where $\sigma_k^z$ is the Pauli operator in the $z$ direction acting on the $k$th molecule. When the sample is in a state of a definitive type \(L\), its bulk
magnetization is equal to \( N(L_1 - L_2) = N(2L - 1) \), which is simply the number of spins pointing up minus the number of spins pointing down. Hence, the observable corresponding to the bulk magnetization can be written as

\[ M^z = N \sum_L (2L - 1) Q_L^{(N)} \]

where the sum is over all types. The type projectors \( Q_L^{(N)} \) are projectors on the degenerated eigensubspaces of the bulk magnetization operator. Clearly, an exact measurement of the magnetization \( M^z \) would reveal the type of the state of the sample, i.e. the relative frequency of up and down spins.

**Coarse grained macroscopic POVMs**

We will now present how finite accuracy macroscopic observables can be expressed in terms of type projectors. Before we do so, we briefly recall some basic concepts of the theory of generalized measurement \([\text{Kra83a}]\). Generalized measurements (POVMs) are described by a set positive operators \( E_j \) summing to identity. The generalized Born rule for the probability of getting outcome \( E_j \) given initial state \( \rho \) is the same as for von Neumann measurements

\[ P(E_j) = Tr\{E_j \rho \}. \tag{3.8} \]

After the measurement outcome \( E_j \) is observed, the state of the system gets updated to

\[ \rho \xrightarrow{\text{j}} \rho_{|j} = \frac{\sum_i A_{ji}^\dagger \rho A_{ji}}{P(E_j)}, \tag{3.9} \]

where the *Kraus operators* \( A_{ji} \) can be any set of operators satisfying \( \sum_i A_{ji} A_{ji}^\dagger = E_j \).

Here, we will often consider *ideal* quantum measurements where the disturbance inflicted to the system is in some sense minimal \([\text{Fuc02c}]\). This restriction is necessary if we want to study the optimal tradeoff between information gathering and state disturbance. To each measurement outcome \( E_j \) of an ideal measurement is associated a *single* Kraus operator \( A_{j0} = \sqrt{E_j} \). In this case, the state update rule Eq.(3.9) simplifies to

\[ \rho \xrightarrow{\text{j}} \rho_{|j} = \sqrt{E_j} \rho \sqrt{E_j} \frac{P(E_j)}{P(E_j)}, \tag{3.10} \]

which reduced to the regular state update rule when \( E_j \) are projection operators. Hence, von Neumann measurements are minimally disturbing POVMs with an extra orthogonality constraint. Any generalized measurement can be realized physically by coupling
3.2. Definitions

the system of interest to a larger system and performing a von Neumann measurement on the larger system; an example of such a physical construction will be presented in Section 3.6. Similarly, any such “indirect” measurement corresponds to a POVM. Hence, POVMs do not add anything extra to plain textbook quantum mechanics, beside conciseness.

Continuing with our example, finite accuracy measurement of the bulk magnetization of a sample of $N$ spin-$\frac{1}{2}$ molecules can be described in terms of coarse-grained type operators $\tilde{Q}_L^{(N)}$. When the state of the sample is of a definite type $L$, the observed value of the bulk magnetization will not necessarily be equal to $N(2L - 1)$ but, due to the uncertainty of the measurement apparatus, may take different values $N(2\ell - 1)$, with respective probabilities $q_L(\ell)$. The function $q_L(\ell)$ should be centered around $L$ and have a certain width $\sigma$ corresponding to the coarseness of the measurement.

Hence, the coarse-grained type measurements can be defined by “smoothing” the exact type projectors:

$$\tilde{Q}_L^{(N)} = \sum_L \sqrt{q_L(\ell)} Q_L^{(N)}$$

(3.11)

where $q_L(\ell)$ is some probability distribution over $\ell$ centered roughly at $L$ and has the interpretation given above. In principle, $\ell$ could be any real $d$-dimensional vector, as it contains statistical fluctuations. For example, $q_L(\ell)$ could be a $d$-dimensional Gaussian

$$q_L(\ell) = \left(\frac{1}{2\pi\sigma^2}\right)^{\frac{d}{2}} \exp\left\{-\frac{\|\ell - L\|_2^2}{2\sigma^2}\right\}$$

(3.12)

which is properly normalized $\int q_L(\ell) d\ell = 1$ and where the $L_2$-norm is $\|\ell - L\|_2^2 = \sum_j (\ell_j - L_j)^2$. The operators $E_\ell = \tilde{Q}_L^{(N)} \tilde{Q}_L^{(N)\dagger}$ form a POVM (with a continuous outcome) since they are all positive operators and satisfy

$$\int E_\ell d\ell = \int \tilde{Q}_L^{(N)} \tilde{Q}_L^{(N)\dagger} d\ell = I.$$  

(3.13)

These coarse-grained type operators describe a situation where our measurement apparatus is not sufficiently precise to measure the exact population of each level, but rather provides an estimation of it within a finite accuracy $\sigma$.

We have assumed that the measurement outcome $\ell$ takes on a continuous spectrum. However, several measurement apparatus, like those equipped with a numerical output display, have a discrete spectrum of outcomes. This can be taken into account by
choosing a smoothing function

\[ q_L(\ell) = \sum_{\ell_j} \delta(\ell - \ell_j) f_j(L) \]

where \( \{\ell_j\} \) is the set of possible outcomes. Thus, we will henceforth consider the more general continuous case, but all our analysis carries through for discrete measurement outcomes by performing the above substitution.

3.3. Type measurement on identically prepared systems

Type projectors were first studied by Finkelstein [Fin63a], Hartle [Har68a], and Graham [Gra73a] as part of discussions on the interpretation of probabilities in quantum theory. The main characteristic of type projectors identified by these authors can be summarized as follows. Let \( |\psi\rangle = \sum_j \beta_j |x_j\rangle \) be an arbitrary pure state of a \( d \)-level molecule, with associated density matrix \( \nu = |\psi\rangle \langle \psi| \). Consider a sample of \( N \) identically prepared molecules, such that the state of the sample is \( |\Psi_N\rangle = |\psi\rangle^\otimes N \). Upon measurement of the type of the sample, we expect a result close to the probability distribution \( R = (\langle x_1|\nu|x_1\rangle, \ldots, \langle x_d|\nu|x_d\rangle) = (|\beta_1|^2, \ldots, |\beta_d|^2) \). Indeed, it follows from the strong law of large numbers that

\[
\lim_{N \to \infty} \left| F_j^{(N)} |\Psi_N\rangle - |\beta_j|^2 |\Psi_N\rangle \right|^2 = 0, \tag{3.14}
\]

where \( F_j^{(N)} \) is the \( j \)th component of the frequency operator defined at Eq.(3.7). In other word, \( F^{(N)} |\Psi_N\rangle = R |\Psi_N\rangle \) with probability one in the limit of infinite \( N \). This led Hartle to the conclusion that an infinite number of identically prepared molecules are in an eigenstate \( |\Psi_\infty\rangle \) of the frequency operator \( F^{(\infty)} \) with eigenvalue \( R \). Finkelstein, on the other hand, concluded from Eq.(3.14) that for finite \( N \), \( |\Psi_N\rangle \) is “close” to an eigenstate of \( F^{(N)} \) with eigenvalue \( R \). Thus, a measurement of the frequency operator reveals the probabilities \( R_j = \langle x_j|\nu|x_j\rangle \), in the standard Copenhagen sense, of observing a single molecule of the sample in the state \( |x_j\rangle \).

However, the conclusions reported above can be quite misleading. There are really two distinct issues here. The first one concerns the validity of the argument as a derivation of Born’s rule to assign probabilities in quantum theory. The main complication comes from the definition of \( F^{(\infty)} \) as the limit of a finite operator. This limit does not uniquely defined the operator on the non-separable Hilbert space \( \mathcal{H}_m \otimes \mathcal{H}_m \otimes \ldots \) of the
infinite sample: specifying the action of $F^{(\infty)}$ on all states of the form $|x_1\rangle \otimes |x_2\rangle \otimes \ldots$ is not enough to define it. This was realized in [FGG89a] where an alternative derivation of the probability rule was presented. Nevertheless, the proposed solution is still not satisfactory as it relies itself on probability theory. An up-to-date and rather critical discussion of the status of the frequency operator and the related programs can be found in a recent paper of Caves and Schack [CS04a]. We will not address these issues any further and do not claim to offer an alternative derivation of Born’s rule.

The second difficulty which is directly relevant to the present study concerns state disturbance. When a system is prepared in an eigenstate of a physical observable, the act of measurement does not disturb it. While Eq.(3.14) does not grant this for any finite $N$, one naturally expects (like Finkelstein did) that, as $N$ grows, the disturbance caused by the measurement should decrease and eventually become negligible for all practical purpose.

In what follows, we will show that the measurement of macroscopic observables induces an important disturbance to the state of the sample. In fact, this disturbance increases as the size $N$ of the sample grows. This is in apparent contradiction with the conclusion that one might intuitively draw from Eq.(3.14) by extending it to finite $N$. However, we will show how the above conclusion can be recovered when the measurement of macroscopic observables are of finite accuracy: sufficiently coarse grained type measurements induce a negligible disturbance to the state of the sample. We are interested in the tradeoff between measurement accuracy and state disturbance.

**State disturbance**

There are several ways to characterize the disturbance caused to the sample by a measurement. For this, we first need to define a few states. Initially, any one molecule of the sample is in the state $\nu$, so the sample itself is assigned the state $\rho_N = \nu^{\otimes N}$. In what follows, we will define the conditional post-measurement state of the sample $\rho_N|\ell$ to be the state of the sample after measurement outcome $\ell$ has been obtained. This state can be compared with the sample’s initial state $\rho_N$ to evaluate the disturbance. Similarly, the conditional post-measurement state of a single molecule of the sample will be denoted $\rho_{1|\ell}$ and should be compared with its original state $\nu$ of a single molecule. One can also consider the (unconditional) post-measurement state of the sample $\rho'_N$. This state should be assigned in a situation where (like is often the case in NMR for
Macroscopic observables

example) a measurement is performed but its outcome is not observed. Hence, \( \rho'_N \) is naturally defined by averaging \( \rho_{N|\ell} \) over measurement outcomes \( \ell \). This situation is also very typical of open systems: the environment “measures” the system, but the information escapes our monitoring. Thus, \( \rho'_N \) and its single molecule analogue \( \rho'_1 \) play a central role in the theory of decoherence.

The state of the sample can be rearranged as follows

\[
|\Psi_N\rangle = \left( \sum_{j=1}^{d} \beta_j |x_j\rangle \right)^{\otimes N} \\
= \sum_{X \in \mathcal{X}^N} \left( \prod_{j=1}^{d} \beta_{j}^{NL_j}(X) \right) |X\rangle \\
= \sum_{L} \left( \prod_{j=1}^{d} \beta_{j}^{NL_j} \right) \sum_{X \in T[L]} |X\rangle \\
= \sum_{L} \left( \prod_{j=1}^{d} \beta_{j}^{NL_j} \right) \sqrt{|T[L]|} |L\rangle
\]

(3.15)

where we have defined the normalized state

\[
|L\rangle = \frac{1}{\sqrt{|T[L]|}} \sum_{X \in T[L]} |X\rangle
\]

and \( |T[L]| = (NL_1,...,NL_d) \) denotes the cardinality of the type class \( T[L] \). The density operator associated to this state will be denoted \( \rho_N = |\Psi_N\rangle \langle \Psi_N| = \nu^{\otimes N} \).

Upon measurement of the coarse-grained operators of Eq.(3.11), the probability of observing an outcome within an infinitesimal volume range \( d\ell \) of \( \ell \) is \( P(\tilde{Q}_\ell^{(N)}) d\ell \) where (see Eq.(3.8))

\[
P(\tilde{Q}_\ell^{(N)}) = Tr \left\{ \tilde{Q}_\ell^{(N)} \rho_N \tilde{Q}_\ell^{(N)} \right\} \\
= \sum_{L,L'} \sqrt{q_L(\ell)q_{L'}(\ell)} Tr \left\{ Q_L^{(N)} \rho_N Q_{L'}^{(N)} \right\} \\
= \sum_{L} q_L(\ell) \langle \Psi_N | Q_L^{(N)} | \Psi_N \rangle \\
= \sum_{L} q_L(\ell) m(L, R)
\]

(3.16)

and \( m(L, R) \) denotes the multinomial distribution \( (NL_1,...,NL_d) \prod_j R_{j}^{NL_j} \). Following Eq.(3.10), the conditional post-measurement state of the ensemble given measurement
outcome $\ell$ is

$$
\rho_{N|\ell} = \frac{\tilde{Q}_\ell^{(N)} \rho_N \tilde{Q}_\ell^{(N)}}{P(\tilde{Q}_\ell^{(N)})} = \sum_L \sum_{L'} \prod_{j,j'} \beta_j^{NL_j} \beta_j^{*NL_j'} q_L^{(\ell)} q_L^{(\ell')} \sqrt{T[L] \cdot |T[L]|} \sum_{L} \sum_{L'} \prod_{j,j'} \beta_j^{NL_j} \beta_j^{*NL_j'} G(L,L') \sqrt{|T[L]| \cdot |T[L']|} \langle L | L' \rangle.
$$

(3.18)

The post-measurement state is obtained by averaging the conditional post-measurement states over all measurements outcomes

$$
\rho'_{N} = \int P(\tilde{Q}_\ell^{(N)}) \rho_{N|\ell} d\ell = \int \tilde{Q}_\ell^{(N)} |\Psi\rangle \langle \Psi| \tilde{Q}_\ell^{(N)} = \sum_L \sum_{L'} \prod_{j,j'} \beta_j^{NL_j} \beta_j^{*NL_j'} G(L,L') \sqrt{T[L] \cdot |T[L']|} \langle L | L' \rangle
$$

(3.19)

where we have defined the decoherence kernel

$$
G(L,L') = \int \sqrt{q_L^{(\ell)} q_L^{(\ell')}} d\ell.
$$

(3.20)

Notice that setting $G(L,L') = 1$ in Eq.(3.19) would yield a density matrix $\rho'_{N}$ identical to $\rho_{N}$. Finally, the post-measurement state of a single molecule of the sample is obtained by taking a partial trace over $N-1$ molecules $\rho'_{1} = Tr_{N-1}\{\rho'_{N}\}$, and similarly for the conditional post measurement state $\rho'_{1|\ell} = Tr_{N-1}\{\rho_{N|\ell}\}$.

The disturbance caused by the measurement is evaluated with the fidelity between the pre- and post-measurement state. A fidelity of 1 indicates that the two states are identical — i.e. the measurement did not cause disturbance — while a fidelity 0 indicates maximal disturbance. The fidelity between two states $\rho$ and $\nu$ is

$$
F(\rho, \nu) = \left( Tr \left\{ \sqrt{\rho \frac{1}{2} \nu \frac{1}{2} \rho^2} \right\} \right)^2.
$$

(3.21)

If one of the state is pure, say $\nu = |\phi\rangle \langle \phi|$, this reduces to the familiar “overlap” $F(\rho, |\phi\rangle \langle \phi|) = \langle \phi | \rho | \phi \rangle$.

It is instructive to first consider the case where the measurement are perfectly accurate, $\sigma = 0$ in Eq.(3.12), which implies $q_L(\ell) = \delta(\ell - L)$ and $G(L,L') = \delta_{LL'}$. In this case, the post-measurement density matrix is

$$
\rho'_{N} = \sum_L m(L,R) |L\rangle \langle L|,
$$

(3.22)
it has completely decohered in the type basis $|L\rangle$, i.e. there are no off-diagonal terms of the form $|L\rangle\langle L'|$ like in Eq. (3.19). The fidelity between the pre- and post-measurement state is then

$$F_{\sigma=0}(\rho_N, \rho'_N) = \sum_L [m(L, R)]^2$$

$$\leq \sum_L m(L, R) \times \left( \max_L m(L, R) \right)$$

$$\approx \frac{1}{(2\pi N)^{d+1} \prod_j |\beta_j|}$$

(3.23)

where the subscript $\sigma = 0$ indicates that the measurement are perfectly accurate, and we have used Stirling’s approximation in the last line. Clearly, exact type measurements greatly disturb the system, since fidelity goes to zero as the size of the sample increases, except in the case where $\beta_j = \delta_{jj}$. A similar conclusion based on different considerations was reached by Squires [Squ90a]. It follows from the concavity of fidelity $F(\rho, \sum_j p_j \nu_j) \geq \sum_j p_j F(\rho, \nu_j)$ that the conditional post-measurement state $\rho_N|\ell$ also has, with high probability, a vanishing fidelity with the original state $\rho_N$.

The disturbance caused by an exact type measurement is most obvious when considering the conditional post-measurement state of a single molecule from the sample. As shown in Appendix B.1,

$$\rho_1|\ell = \sum_{j=1}^d \ell_j|x_j\rangle\langle x_j| :$$

(3.24)

the conditional post-measurement state of a single molecule is diagonal in the $|x_j\rangle$ basis with eigenvalues given by the observed type of the sample $\ell$, independently of its state $\nu$ prior to the measurement. In words, an ensemble measurement of the relative occupation number of the single-molecule states $\{|x_j\rangle\}$ with outcome $\ell = (\ell_1, \ell_2, \ldots, \ell_d)$ “resets” the reduced state of a single molecule to a statistical mixture of the states $\{|x_j\rangle\}$ with associated probabilities $\ell_j$. However, following the typical sequence theorem Eq. (3.1), the observed coefficients $\ell_j$ are very likely to be close to $R_j = \langle x_j|\nu|x_j\rangle$. When averaging over measurement outcomes, we recover the state $\nu \rightarrow \rho_1|\ell = \sum_j R_j|x_j\rangle\langle x_j| which has no off-diagonal terms, i.e. $|x_i\rangle\langle x_j|$. Thus, the exact measurement of a macroscopic observable completely decoheres individual molecules of the sample; it leaves the diagonal elements of $\nu$ unchanged while suppressing all off-diagonal terms. (This situation
might appear worrisome for bulk-ensemble quantum computing; we will return to this in Section 3.6). Moreover, the measurement creates correlation between the molecules, so \( \rho_N' \neq (\rho_1')^\otimes N \) and \( \rho_{N|\ell}' \neq (\rho_{1|\ell})^\otimes N \) in general. The conditional post-measurement state \( \rho_{N\ell}' \) can even have entanglement across the different molecules of the sample.

### Gaussian smoothing

We now turn our attention to the case where the smoothing function \( q_L(\ell) \) has a finite width \( \sigma \). In the case of interest, the initial state of the sample \( |\Psi_N\rangle \) is pure, so combining Eqs. (3.15) and (3.19) we get

\[
F(\rho_N, \rho_N') = \langle \Psi_N | \rho_N' | \Psi_N \rangle
= \sum_{L, L'} m(L, |\beta_j|^2) m(L', |\beta_j|^2) G(L, L').
\] (3.25)

For sake of clarity, we will first consider the Gaussian distribution \( q_L(\ell) \) defined at Eq. (3.12). The decoherence kernel defined at Eq. (3.20) is then given by

\[
G(L, L') = \int \left( \frac{1}{2\pi\sigma^2} \right)^{\frac{d}{2}} e^{-\frac{\|\ell - L\|^2 + \|\ell - L'\|^2}{4\sigma^2}} d\ell
= \exp \left\{ -\frac{\|L - L'\|^2}{2(2\sigma)^2} \right\}.
\]

This is not surprising as the decoherence kernel is the convolution of the smoothing function with itself. The convolution of two distribution of width \( \sigma_1 \) and \( \sigma_2 \) gives a distribution of width \( \sigma' = \sigma_1 + \sigma_2 \), so \( G(L, L') \) is a function of width \( 2\sigma \).

We can find a lower bound to the fidelity by truncating the sum in Eq. (3.25). By restricting \( L \) and \( L' \) to the domain \( D = \{ L : \|L - R\|_2 \leq \Delta \} \) where \( R_j = \langle x_j | \nu | x_j \rangle \), we can lower bound the kernel by \( G(L, L') \geq \exp\left\{ -\frac{\Delta^2}{2\sigma^2} \right\} \) using the triangle inequality. This yields the inequality

\[
F(\rho_N, \rho_N') \geq \exp \left\{ -\frac{\Delta^2}{2\sigma^2} \right\} \left( \sum_{L \in D} b(L) \right)^2.
\]

The quantity in the parenthesis is a sum over the range \( D \) of a multinomial probability distribution. It is equal to \( P(||L - R||_2 \leq \Delta) \geq P(||L - R||_1 \leq d\Delta) \geq (1 - e^{-Nd\Delta^2/2}) \) by the Cauchy-Schwartz inequality, c.f. Proposition A.0.1, and the typical sequence theorem Eq. (3.1). Thus, we get

\[
F(\rho_N, \rho_N') \geq \exp \left\{ -\frac{\Delta^2}{2\sigma^2} \right\} \left( 1 - e^{-Nd\Delta^2/2} \right)^2.
\] (3.26)
Since this bound holds for all $\Delta$ (which is an arbitrary cut-off), we can maximize the RHS of Eq. (3.26) — the optimal value turn out to be attained when $\Delta^2 = 2 \ln(1+2N\sigma^2d)/Nd$ — to get the tightest bound:

$$F(\rho_N, \rho_N') \geq 1 - \frac{1 + \ln(2N\sigma^2d)}{N\sigma^2d}. \quad (3.27)$$

Hence, as the size of the sample increases, the measurement accuracy $\sigma$ can decrease as fast as $1/\sqrt{N}$ while maintaining a constant fidelity $F(\rho_N, \rho_N') = 1 - \epsilon$ between the pre- and post-measurement states. If $\sigma$ decreases less rapidly than $1/\sqrt{N}$, e.g. $N^{-s}$ for $0 < s < 1/2$, the fidelity will go to 1 as $N$ grows. In particular, if $\sigma$ is constant, $F(\rho_N, \rho_N') \sim 1 - c \ln N$.

The fidelity between the pre- and conditional post-measurement state, i.e. $\rho_N$ and $\rho_{N|\ell}$ respectively, can be computed using similar techniques. The computation is illustrated in Appendix B.2. While the mathematical details are slightly more involved, the essence of the result is identical: as long as $\sigma \gg 1/\sqrt{N}$ — i.e. $\sigma = N^{-s}$ for $0 \leq s < 1/2$ — the fidelity $F(\rho_N, \rho_{N|\ell})$ goes to 1 as $N$ increases. Moreover, this is true independently of the measurement outcome $Q^{(N)}_\ell$, in contrast with the result obtained in Ref. [BHL04a], where a low fidelity was obtained with some small probability.

**General smoothing**

We now wish to argue that the essence of our measurement accuracy-state disturbance tradeoff applies to arbitrary smoothing function $q_L(\ell)$ introduced at Eq. (3.11), provided that it is actually smooth with respect to $L$. Let us be more precise. Intrinsic to the smoothing function is a notion of distance on the $d$-dimensional probability simplex. One can define various distance measures on this space, e.g. our choice of smoothing function Eq. (3.12) in the previous section relied on the distance $\|L - L\|_2$ induced by the $L_2$-norm. The exact statement of the tradeoff will obviously depend on the choice of distance measure. However, the essence of the result is independent of this choice, as all good distance measure are equivalent on small distances. Thus, a good smoothing function $q_L(\ell)$ should satisfy

$$|q_L(\ell) - q_{L'}(\ell)| \leq c \left(\frac{\|L - L\|_1}{\sigma}\right)^s \quad (3.28)$$

for sufficiently small $\|L - L\|_1$ and some positive constants $c$ and $s$ (Eq. (3.28) is known as Lipschitz condition). In general, $c$ depends on the dimension $d$ of the molecules.
Therefore, the dependence of the bound Eq. (3.27) on the dimension $d$ (which may seem awkward) only reflects our choice of the $L_2$-norm in the smoothing function, it is not universal. Given this assumption, we can derive the general result. It should be mentioned that ultimately, $q_L(\ell)$ depend on the details of the measurement procedure of the corresponding macroscopic observable (see for example the model of Section 3.6). However, if this measurement is of finite accuracy, then the smoothing function must have a certain width and should satisfy the above assumption.

We see from Eq. (3.25) that fidelity between the pre- and post-measurement state only depends on the decoherence kernel $G(L, L') = \int \sqrt{q_L(\ell)q_{L'}(\ell)}d\ell$. Thus, the procedure used in the previous section carries through straightforwardly. We can truncate the sum Eq. (3.25) to the domain $\mathcal{D}$ where $\|L - R\|_1 \leq \Delta$, with $R_j = |\beta_j|^2$. On this domain, the fluctuations of the kernel are bounded by Eq. (3.28) using the triangle inequality. Moreover, as $G(L, L) = 1$ by the normalization condition of the smoothing function, we obtain

$$G(L, L') \geq 1 - c(\Delta/\sigma)^s$$

on $\mathcal{D}$.

The bound

$$F(\rho_N, \rho'_N) \geq \left\{ 1 - c \left( \frac{\Delta}{2\sigma} \right)^s \right\} \left( 1 - e^{-N\Delta^2/2} \right)^2.$$ \hspace{1cm} (3.29)

follows straightforwardly from the typical sequence theorem Eq. (3.1). Given the value of $c$ and $s$, one can perform an optimization with respect to $\Delta$ to get the tightest bound. However, this depends on the details of the smoothing function.

Similarly, we can derive a bound for the fidelity of the conditional post-measurement state when $\sigma \gg 1/\sqrt{N}$. The technique illustrated in Appendix B.2 for a specific choice of smoothing function can indeed be applied straightforwardly to any type of smoothing function satisfying Eq. (3.28). The basic steps, starting from the expression

$$F(\rho_N, \rho_{N|\ell}) = \frac{\left( \sum_L \sqrt{q_L(\ell)m(L, R)} \right)^2}{\sum_L q_L(\ell)m(L, R)}$$

are the following. The sum in the nominator is truncated to the domain $\mathcal{D}$. Using the typical sequence Theorem and Eq. (3.28), we get

$$\left( \sum_L \sqrt{q_L(\ell)m(L, R)} \right)^2 \geq (q_R(\ell) - c(\Delta/\sigma)^s) \left( 1 - e^{-N\Delta^2/2} \right)^2.$$
Macroscopic observables

Figure 3.1: State disturbance for a general smoothing function. The smoothing function (red) varies very slowly on the domain where the density operator has a non negligible support (green). Indeed, the width of the multinomial \( m(L, R) \) scales as \( 1/\sqrt{N} \). On this domain, the variation of the smoothing function (or of the decoherence kernel) is bounded by \( c/\sqrt{N}\sigma \), which dictates the state disturbance.

The denominator is bounded by Eq. (3.28)

\[
\sum_L q_L(\ell) m(L, R) \leq q_R(\ell) + c(\Delta/\sigma)^s.
\]

Combining these two inequalities yields, to first order

\[
F(\rho_N, \rho_N|\ell) \geq 1 - 2c(\Delta/\sigma)^s - 2e^{-N\Delta^2/2}.
\]

Again, the free parameter \( \Delta \) should be optimized to find the tightest bound; the details of the tradeoff depend on the form of the smoothing function. The general idea behind the proof can also be understood intuitively from Fig. 3.1.

Finally, the scaling \( \sigma \sim 1/\sqrt{N} \) is optimal. A higher precision would considerably disturb the state of the system. This is because the multinomial distribution \( m(L, R) \) has a width \( 1/\sqrt{N} \). Consider the expression of Eq.(3.25). If the kernel has a width smaller than the binomial distribution, the sum, and hence the fidelity \( F(\rho_N, \rho'_N) \), will be roughly equal to \( \text{erf}(\sigma\sqrt{N}) \approx 2\sigma/\sqrt{N\pi} \) for \( \sigma \ll 1/\sqrt{N} \). The bound is also tight for the conditional post-measurement fidelity \( F(\rho_N, \rho_N|\ell) \) as fidelity is a convex function. This can also be seen intuitively by considering the behavior of two consecutive
measurements. Upon fine grained measurement $Q^{(N)}_L$, the variance of the outcome $L$ is $1/\sqrt{N}$. However, if we first perform a coarse grained measurement $\tilde{Q}^{(N)}_\ell$ of width $\sigma \ll 1/\sqrt{N}$ and then perform a fine grained measurement on the updated state $\rho_{N|\ell}$, the variance of the second measurement outcome will be $\sigma$: performing the coarse grained measurement has altered its statistics. This means that the coarse grained measurement has appreciably disturbed the state of the sample, so $F(\rho_N, \rho_{N|\ell})$ is far from 1.

**Mixed states**

The results established in the present Section hold unchanged when the molecules of the sample are all prepared in the same mixed state $\nu = \sum_{i=1}^d \lambda_i |\psi_i\rangle \langle \psi_i|$. The argument proceeds in three steps. First, we can construct a purification of the state $\nu$ by appending to each molecule an ancillary system of dimension $d$ with orthonormal basis $\{|i\rangle\}$. Clearly, the reduced state of the molecule — obtained by tracing out the ancilla — is $Tr_{\text{ancilla}}\{|\phi\rangle\langle \phi|\} = \nu$. Second, the vectors $\{|x_j\rangle|i\rangle\}$ form a basis for the Hilbert space of the pair molecule+ancilla. The type projectors $Q^{(N)}_L$ associated to the molecule only measure the type of the prefix $x_j$, so are coarse grained version of the type projectors associated to the pair: the disturbance they cause to the state of the sample can only be less than the disturbance caused by the complete type projectors. Thus, the bound Eq.(3.26) can be applied to $F(\Phi_N, \Phi'_N)$ where $\Phi_N = |\phi\rangle\langle \phi| \otimes \mathbb{1}^N$, and

$$\Phi'_N = \int (\tilde{Q}^{(N)}_\ell \otimes \mathbb{1}) \Phi_N (\tilde{Q}^{(N)}_\ell \otimes \mathbb{1}) d\ell.$$

Finally, by monotonicity of the fidelity — $F(\mathcal{E}(\rho), \mathcal{E}(\nu)) \geq F(\rho, \nu)$ for any trace preserving quantum operation $\mathcal{E}$ — the bound applies directly to the pre- and post-measurement state of the sample of molecules by tracing out the ancillas. By similar considerations, all of the above conclusions can be extended to mixed states.

### 3.4. Exchangeability

Before proceeding with the applications of the above results, we present an important result that will — under certain assumptions — lead to the emergence of an inter-
subjective agreement among independent observers about the state of macroscopic systems. The concept of *exchangeability* was introduced in the classical theory of probability by de Finetti [deF90a] to substitute the incorrect use of “unknown probabilities” by a concept that makes sense. A probability assignment is the expression of one’s subjective knowledge about the possible outcomes of an experiment. Hence, it is not a property of a physical system itself but, rather, a property of the observer assigning the probability, so it can not be unknown to him!

As discussed in Chapter 1, there are also several good reasons to believe that quantum states are subjective, see for example [CF96a, FP00a, Mer01a, CFS02a, Fuc02c, Spe04a] and references therein.\(^2\) As a consequence, the concept of an *unknown quantum state* is in general an oxymoron, for essentially the same reasons which lead to this conclusion for classical probability assignment.

However, unknown quantum states turn out to be quite useful for the description of certain physical settings. Of particular interest to us is the description of a sample of \(N\) “molecules”. Under certain circumstances — e.g. thermal equilibrium — one can arrive at the conclusion that all the molecules of the sample are equivalent, so they should all be describe by the same state \(\nu\), which is itself unknown. This is a very common state of affairs in nuclear, atomic, or molecular physics where spectral quantities — which are formally described by macroscopic observables — are measured over a large collection of quantum systems. In fact, in almost all physical experiments where ensemble measurements are performed, the components of the sample are assumed to be in the “same unknown state”, and the purpose of the measurement is to (partially) determine this state. Moreover, note that macroscopic observables do not allow one to discriminate between the molecules: all molecules of the sample are treated on equal footing. Hence, information gathered by macroscopic measurements naturally lead to a state assignment where all molecules are in the same, but perhaps partially unknown, state.

To arrive at an appropriate description of the sample without refering to the unknown quantum state of individual molecules, we must clearly state the assumption of the observer assigning the state. His assumption is that *the arbitrary number of molecules are all equivalent*, which can be formalized by demanding that the state \(\rho_N\)

\(^2\)To quote Robert Griffiths, “If probabilities are not real, then pre-probabilities [quantum states] are even less real” [Gri04a].
assigned to the sample by the observer satisfies the following requirements:

1. For any permutation $\pi$ of the $N$ molecules, $\pi[\rho_N] = \rho_N$. Such a state is called symmetric.

2. For any positive integer $M$, there exists a symmetric state $\rho_{N+M}$ such that $\rho_N = Tr_M\{\rho_{N+M}\}$, where $Tr_M$ denotes the partial trace over $M$ molecules.

A state $\rho_N$ satisfying these two conditions is called exchangeable. The quantum de Finetti representation theorem [HM76a, Hud81a, CFS02b] asserts that any exchangeable quantum state $\rho_N$ of a sample of $N$ molecules can be written as

$$\rho_N = \int \nu^\otimes N Pr(\nu) d\nu$$

where $\nu$ are density operators of a single molecule and $Pr(\nu)$ is a probability distribution over the quantum states of a single molecule.

The interpretation of this theorem is that it is mathematically correct to look upon $\nu$ as an objective element of reality about which we have incomplete knowledge: hence we assign it some probability distribution $Pr(\nu)$. For example, when the POVM $\{E_i\}$ is measured on the sample, the outcome $E_j$ is observed with probability

$$P(E_j) = Tr\{E_j \rho_N\} = \int Tr\{E_j \nu^\otimes N\} Pr(\nu) d\nu = \int P(E_j | \nu^\otimes N) Pr(\nu) d\nu.$$ \hspace{1cm} (3.31)

We can think of $P(E_j | \nu^\otimes N)$ as the probability of $E_j$ given a value of the real parameter $\nu$, but since $\nu$ is unknown, we average this probability over the possible values of $\nu$ distributed according to $Pr(\nu)$. Note the complete similarity between Eq. (3.31) and the prior probability of data $D$ measured on a classical system Eq. (1.2), which is the average of the probability $P(D | x, p)$ of $D$ given that the system occupies the “objective” coordinates $(x, p)$, averaged over all coordinates. However, it must be emphasized that it is the assumption of exchangeability which leads to the form of Eq. (3.30), which in turn legitimizes the term “unknown state” for mathematical convenience.

**Bulk tomography**

Quantum state tomography is an experimental procedures which transforms an exchangeable state of the form Eq.(3.30) to a product state $\rho = \nu^\otimes N$ through repeated
Macroscopic observables

state updates. According to the de Finetti representation theorem, we can equivalently say — and this is how tomography is conventionally formulated — that the purpose of tomography is to determine which is the real yet unknown state $\nu$ describing the $N$ molecules of the sample.

In [CFS02b], quantum state tomography was studied in the context where the molecules of the sample are measured individually and the state of the rest of the sample was updated. Here, we present how quantum state tomography can be performed through bulk measurements. A similar description was recently and independently developed in [BHL04a]. Let $A_N = \sum_k a(k)$ be a macroscopic observable deriving from the single-molecule observable $a$ as in Eq. (3.2). Exceptionally, we denote the eigenstates and eigenvalues of $a$ with a superscript $a| x^{(a)}_j \rangle = \alpha^{(a)}_j | x^{(a)}_j \rangle$ for later convenience. The finite accuracy measurement of the macroscopic observable $A_N$ is defined through the POVM $\{\tilde{Q}^{(N,a)}_{\ell}\}$.

The conditional state of the sample after the measurement of $\{\tilde{Q}^{(N,a)}_{\ell}\}$ with outcome $\ell^{(a)}$ is

$$\rho_{N|\ell^{(a)}} = \int \left( \tilde{Q}^{(N,a)}_{\ell} \nu \otimes N \tilde{Q}^{(N,a)}_{\ell} \right) \frac{Pr(\nu)}{P(\tilde{Q}^{(N,a)}_{\ell})} d\nu.$$ 

The quantity in parenthesis is proportional to the conditional post-measurement state of the sample, given that it was initially in state $\nu \otimes N$. As demonstrated in Section 3.3, this measurement has very high fidelity with the original state. Mathematically, this means

$$\tilde{Q}^{(N,a)}_{\ell} \nu \otimes N \tilde{Q}^{(N,a)}_{\ell} \approx P(\tilde{Q}^{(N,a)}_{\ell}|\nu \otimes N) \nu \otimes N.$$ 

Therefore, we get

$$\rho_{N|\ell^{(a)}} \approx \int \nu \otimes N \frac{Pr(\nu)P(\tilde{Q}^{(N,a)}_{\ell}|\nu \otimes N)}{P(\tilde{Q}^{(N,a)}_{\ell})} d\nu.$$ (3.32)

Comparing this updated state with the initial state of the sample Eq. (3.30), it is as if we had updated the probability distribution $Pr(\nu)$ of the real yet unknown state $\nu$ according to Bayes’ rule $P(y|x) = P(x|y)P(y)/P(x)$. However, this is strictly a mathematical identity, all we did was to apply the state update rule Eq. (3.9) to an exchangeable state. This is of capital importance. Given the exchangeability assumption and given that the observer can only gather information through the measurement of macroscopic quantities, the quantum state update of Eq. (1.3) behaves just like the classical rule Eq. (1.1). For these observers, the sample behaves as if the reduced state of a single
molecule $\nu$ was an objective element of reality: $\nu$ plays the role of the classical phase space coordinates $(x, p)$ in Eq. (1.1). Hence, the usual experimentalist’s objection to the subjective nature of quantum states “Of course quantum states are real, I measure them in my lab!” is mathematically justified by his limitations to measure macroscopic observables on exchangeable states (or more generally on states with no entanglement on macroscopic scales as we shall soon establish).

We can repeat the procedure with a different macroscopic observable $B_N, C_N, \ldots$ derived from the single-molecule observable $b, c, \ldots$, which do not necessarily commute with each other. If the sets of observables are sufficiently informative — i.e. if their eigenstates $\{|x_j^{(\mu)}\rangle|x_j^{(\mu)}\rangle\}_{\mu=a,b,c,...}$ contain $d^2 - 1$ linearly independent elements — the updated probability distribution will converge with very high probability to a delta function for sufficiently large $N$, $Pr(\nu|\ell^{(a)}, \ell^{(b)}, \ldots) \approx \delta(\hat{\nu})$, so the final state will be $\rho_N|\ell^{(a)}\rangle|\ell^{(b)}\rangle \approx \hat{\nu}^\otimes N$. This is because the functions $P(\hat{Q}_k^{(N,\mu)}|\nu^\otimes N)$ are centered around $\ell^{(\mu)} = (\langle x_1^{(\mu)}|\nu|x_1^{(\mu)}\rangle, \langle x_2^{(\mu)}|\nu|x_2^{(\mu)}\rangle, \ldots)$ and have a width $\sigma$. The state $\hat{\nu}$ is the only one satisfying all the linear constraints $\langle x_j^{(\mu)}|\hat{\nu}|x_j^{(\mu)}\rangle = \ell_j^{(\mu)}$ for all $\mu = a, b, c, \ldots$ up to accuracy $\sigma$. Again, this is as if the measurements simply inform us of the identity of the “real but unknown” $\hat{\nu}^\otimes N$, without disturbing it in the limit of large $N$.

3.5. Classicality

We have seen at the end of the last Section that — under the exchangeability assumption — macroscopic observables behave as classical. Our goal here is to formalize as well as extend this result. Let us first briefly recapitulate the discussion of Chapter 1 from a slightly different angle in order to introduce the main ideas of consistent histories. Observations play very different roles in classical and quantum theory. In the classical setting, we can think of measurements as unveiling an underlying “real” state of affairs: observations reveal information about the objective state of the world without affecting it. On the other hand, quantum measurements disturb or “collapse” the state of the system.

When states, either quantum or classical, are regarded as subjective judgments of the world, both of the above descriptions need revision. Let $P(x_i, y_j)$ be the joint probability distribution, or state, that the observer assigns to the classical sequence of events $X = x_i$ and $Y = y_j$. Upon the observation $X = x_i$, the observer updates his
predictions for event $Y$ according to Bayes’ rule
\[ P(y_j|x_i) = \frac{P(x_i,y_j)}{P(x_i)} \]
where $P(x_i) = \sum_j P(x_i,y_j)$. This state generally differs from the pre-measurement state assigned to $Y$
\[ P(y_j|x_i) \neq P(y_j) = \sum_i P(x_i,y_j). \]
Hence, the act of observing $X$ modifies the state assigned to $Y$. However disregarding the observed value of $X$ for later probability assignments is like not measuring the value of $X$ at all:
\[ P(y_j) = \sum_i P(y_j|x_i)P(x_i). \quad (3.33) \]
Indeed, we can interpret the observation as revealing the “real” value of $X$ which was there all along: the observer simply didn’t know about it prior to his observation. In this sense, $X = x_i$ is a real state of affairs about which the observer learns through the act of measurement. Thus, the state he assigns to $Y$ prior to his observation of $X$ is the mixture of the state it would have given the different value of $X$, weighted by the probability of $X$, c.f. Eq. (3.33) and Eq.(1.1). This reasoning extends in an obvious way to any sequence of events $X^{(1)}, X^{(2)}, \ldots, X^{(n)}$. We can consider that the system follows a fixed history $x^{(1)}_{j_1}, x^{(2)}_{j_2}, \ldots, x^{(n)}_{j_n}$ of which the observer has incomplete knowledge, resulting in a joint distribution $P(x^{(1)}_{j_1}, x^{(2)}_{j_2}, \ldots, x^{(n)}_{j_n})$.

Quantum measurements behave quite differently. A quantum event corresponds to a “click” on a measurement apparatus at some instant of time $t$. Hence, each event is associated a POVM element $E^{(k)}_{j_k}(t_k)$ in the Heisenberg picture at a given time $t_k$. (We will henceforth drop the explicit time label $t_k$.) In general, assigning definite yet unknown outcomes to these events leads to incorrect predictions, e.g. the sum rule
\[ P(E^{(2)}_{j_2}) = \sum_{j_1} P(E^{(2)}_{j_2}|E^{(1)}_{j_1})P(E^{(1)}_{j_1}) \]
do not hold in general. This is most obvious in Young’s double slit experiment where the events $E^{(1)}_{j_1}$ correspond to the particle going through slit $j_1 = 1$ or $2$ and $j_2$ labels the various positions on the detector. Reasonings involving the particle going through a definite yet unknown slit lead to incorrect predictions.

There are however sequences of quantum events which do behave classically, as if the observations were revealing an underlying reality, the typical example being when all the
POVM elements describing the events commute. The consistent histories approach to quantum theory [Gri84a, GH90a, Omn92a, GO99a] lays down a set of conditions under which such behavior occurs. A complete list of alternative events $\zeta^{(k)} = \{E_{jk}^{(k)}\}$ at time $t_k$ defines a POVM. A history is a list of POVM elements $H = (E_{j1}^{(1)}, E_{j2}^{(2)}, \ldots, E_{jn}^{(n)})$ at distinct times $t_1, t_2, \ldots, t_n$. When the initial state of the system is $\rho$, the probability of an history $H$ is

$$P(H) = \text{Tr} \left\{ (E_{jn}^{(n)})^{\frac{1}{2}} \cdots (E_{j1}^{(1)})^{\frac{1}{2}} \rho (E_{j1}^{(1)})^{\frac{1}{2}} \cdots (E_{jn}^{(n)})^{\frac{1}{2}} \right\} \quad (3.34)$$

following Eqs.(3.8,3.10). A complete family of histories is the set of all combination of POVM elements from the sets $\zeta^{(k)}$ at all times, $\mathcal{F} = \{\zeta^{(1)}, t_1; \zeta^{(2)}, t_2; \ldots, \zeta^{(n)}, t_n\}$. One can regroup histories into coarser descriptions of the sequence of events by taking their unions, e.g. $H = H_1 \cup H_2$. A complete family of histories is thus a sample space on which a probability distribution $P(H)$ is defined. The family is said to be consistent when the sum rule approximately holds for $P(H)$. This condition is the simplest version of all consistency conditions but will be sufficient for our purposes. In this sense, consistent histories define a quasiclassical domain of familiar experience.

As was observed by Halliwell [Hal98a, Hal99a], histories corresponding to a sequence of finite accuracy measurement of macroscopic observables generate a consistent family if the system is a sufficiently large sample of identically prepared molecules, i.e. when $\rho = \nu \otimes N$. It should be stressed that the single-molecule observables $a, b, c, \ldots$ making up the histories do not need to commute. For example, the coarse measurement of the magnetization of a sample of spin-$\frac{1}{2}$ along the $z$ axis followed by a measurement along the $y$ axis can generate a consistent family if the sample is sufficiently large.

A simple argument to build our intuition in this direction is to consider the commutator of any two normalized macroscopic observables. Let $a$ and $b$ be two arbitrary single-molecule observables and define $c$ to be their commutator $c = [a, b]$. These operators can be suitably normalized so that they satisfy $\|a\|, \|b\|, \|c\| \approx 1$. The normalized macroscopic observable $A_N$ is defined as $A_N = \frac{1}{N} \sum_{k=1}^{N} a_{(k)}$, and similarly for $B_N$ and $C_N$; hence $\|A_N\|, \|B_N\|, \|C_N\| \approx 1$. A straightforward calculation shows that the commutator of the normalized macroscopic observables obeys

$$[A_N, B_N] = \frac{1}{N} C_N, \quad (3.35)$$

We assume for simplicity that the POVM are ideal, see Section 3.2.2.
which implies $\| [A_N, B_N] \| \approx \frac{1}{N}$. Thus, all macroscopic observables commute in the limit of infinite-size sample, and commuting observables systematically generate consistent histories: measuring the value of one observable does not affect the outcome statistics of other commuting observables.

However, the infinite-sample considerations can not be applied straightforwardly to finite ensembles (this is the recurrent theme of this Chapter!) In particular, Eq. (3.35) does not involve any coarseness, which is essential to achieve consistency in finite ensembles. Our analysis of Section 3.3 provides the right tools to formally study the consistency of macroscopic histories operating on finite ensembles. Indeed, Halliwell’s is a straightforward consequence of the fact that these measurements leave the state $\nu^{\otimes N}$ of the ensemble essentially unchanged, so they do not alter the statistics of subsequent measurement outcomes. Moreover, our general analysis will allow us to extend the conclusions reached by Halliwell to a much wider set of initial states.

The first generalization is straightforward: by linearity of Eq. (3.34), such families are automatically consistent for initial exchangeable states. Indeed, for initial exchangeable state $\rho_N$ of the form Eq. (3.30), the probability of history $H$ reads

$$P(H) = \int P(H|\nu^{\otimes N}) Pr(\nu) d\nu. \quad (3.36)$$

Clearly, if the sum rule is satisfied for the $P(H|\nu^{\otimes N})$ individually, it is also satisfied for their convex combination. This is very much in the spirit of the de Finetti representation theorem as one can interpret the outcome of the macroscopic measurements as revealing partial information about the real quantum state $\nu^{\otimes N}$ of the sample, of which we have incomplete knowledge. The consistency of such “macroscopic histories” for initial exchangeable state can also be seen as a consequence of the fact that in those conditions, the quantum state update behaves approximately like Bayesian update, c.f. Eq. (3.32). Indeed, the identity $P(x) = \sum_y P(x|y) P(y)$ of classical probability theory (or more precisely its continuous version) applied to Eq. (3.32) implies that the average post-measurement state of the sample is approximately equal to the initial state, $\rho'_N = \int \rho_N|\mathbf{a} d(\mathbf{a}) P(\tilde{Q}^{(N,a)}_\mathbf{a}) d\mathbf{a} \approx \rho_N$ for any initial exchangeable state $\rho_N$. To use the language of Chapter 1, quantum states of the form $\nu_0^{\otimes N}$ play the role of “states of complete knowledge”. Indeed, such states are exchangeable states with the special property that $Pr(\nu) = \delta(\nu - \nu_0)$ (the distribution $Pr(\nu)$ appears in the definition of exchangeable states Eq. (3.30)). Thus, they are not affected by Bayesian updating.
Moreover, consider an arbitrary product state of the sample $\rho = \nu_1 \otimes \nu_2 \otimes \ldots \otimes \nu_N$. We will construct a state $\overline{\nu}^{\otimes N}$ whose measurement outcomes, for coarse grained macroscopic observables, are statistically indistinguishable from those obtained from the product state $\rho$. This will prove that Haliwell’s result applies to arbitrary product states as well. Consider the symmetrized version of $\rho$:

$$\Pi[\rho] = \frac{1}{N!} \sum_{\pi} \nu_{\pi(1)} \otimes \nu_{\pi(2)} \otimes \ldots \otimes \nu_{\pi(N)}$$

where the sum is over all permutations of $N$ elements. The reduced state of a single molecule is

$$\text{Tr}_{N-1}\{\Pi[\rho]\} = \frac{1}{N} \sum_{k=1}^{N} \nu_k = \overline{\nu}. \quad (3.37)$$

The states $\Pi[\rho]$ and $\overline{\nu}^{\otimes N}$ are in some sense very similar: they are both symmetric, they yield the same reduced single-molecule state $\overline{\nu}$, and yield the same expectation value of the frequency operator $\langle F^{(N)} \rangle = (\langle x_1 | \overline{\nu} | x_1 \rangle, \langle x_1 | \overline{\nu} | x_1 \rangle, \ldots)$. However, they are not identical. To illustrate this, consider a sample of $N$ two-dimensional molecule in the state

$$\rho = |x_1\rangle \langle x_1| \otimes \ldots \otimes |x_1\rangle \langle x_1| \otimes |x_2\rangle \langle x_2| \otimes \ldots \otimes |x_2\rangle \langle x_2| ;$$

half of the molecules are in the state $|x_1\rangle$ while the other half are in state $|x_2\rangle$. The measurement of the frequency operator $F^{(N)}$ of Eq.(3.7) yields outcome $(\frac{1}{2}, \frac{1}{2})$ with certainty when the state of the system is $\Pi[\rho]$. The average single molecule state is $\overline{\nu} = \frac{1}{2} |x_1\rangle \langle x_1| + \frac{1}{2} |x_2\rangle \langle x_2|$, so $\overline{\nu}^{\otimes N}$ also yields an average result $(\frac{1}{2}, \frac{1}{2})$ of the frequency operator. But as opposed to the state $\Pi[\rho]$, the outcome of the measurement of $F^{(N)}$ can fluctuate away from $(\frac{1}{2}, \frac{1}{2})$ when the sample is in state $\overline{\nu}^{\otimes N}$. However, according to the typical sequence theorem Eq.(3.1), the size of these fluctuations will be of order $1/\sqrt{N}$, so can only be perceived by macroscopic measurements of accuracy $\sigma \lesssim 1/\sqrt{N}$. For macroscopic observables of coarseness $\sigma \gg 1/\sqrt{N}$, the two states $\Pi[\rho]$ and $\overline{\nu}^{\otimes N}$ will yield the same statistics up to order $\sigma \sqrt{N} \ll 1$.

Moreover, the states $\rho$ and $\Pi[\rho]$ yield exactly the same statistics for measurement outcome of macroscopic observables: this follows straightforwardly from the permutation invariance of the type projectors Eq.(3.4). We have thus established the chain of equality

$$P(\tilde{Q}_k^{(N)} | \rho) = P(\tilde{Q}_k^{(N)} | \Pi[\rho]) \approx P(\tilde{Q}_k^{(N)} | \overline{\nu}^{\otimes N}),$$
so the states \( \rho \) and \( \nu^\otimes N \) yield almost identical predictions when \( \sigma \gg 1/\sqrt{N} \). It follows that a sequence of finite accuracy macroscopic measurements performed on a state of the form \( \rho = \nu_1 \otimes \nu_2 \otimes \ldots \otimes \nu_N \) generate a consistent family of histories for sufficiently large samples. This simple result can be summarized as follows: when the sample is assigned a state \( \rho = \nu_1 \otimes \nu_2 \otimes \ldots \otimes \nu_N \), coarse grained macroscopic measurements behave — to a high accuracy — as if the average state of the molecules \( \bar{\nu} = \frac{1}{N} \sum_j \nu_j \) was an objective element of physical reality being discovered.

In fact, any separable state leads to consistency of macroscopic histories. Indeed, when the molecules of the sample are not entangled with each other, their state can be written as

\[
\rho = \int \nu_1 \otimes \nu_2 \otimes \ldots \otimes \nu_N \Pr(\nu_1, \nu_2, \ldots, \nu_N) d\nu_1 d\nu_2 \ldots d\nu_N. \tag{3.38}
\]

(This is the definition of entanglement: a state is said to be entangled if it cannot be written as Eq. (3.38).) Now, consider the state

\[
\bar{\rho} = \int \bar{\nu}^\otimes N \Pr(\bar{\nu}) d\bar{\nu} \tag{3.39}
\]

where we have defined

\[
\Pr(\bar{\nu}) = \int \Pr(\nu_1, \ldots, \nu_N) \delta\left(\bar{\nu} - \frac{1}{N} \sum_k \nu_k\right) d\nu_1 \ldots d\nu_N.
\]

By linearity and using the result established above, we have \( P(H|\rho) \approx P(H|\bar{\rho}) \) provided that the histories \( H \) are generated by macroscopic observable of accuracy \( \sigma \gg 1/\sqrt{N} \). Since \( \bar{\rho} \) is exchangeable, the probabilities \( P(H|\bar{\rho}) \), and therefore the probabilities \( P(H|\rho) \), approximately satisfy the sum rule. Again, this has a simple interpretation. The average state of the sample \( \bar{\nu} \) behaves like an objective element of reality. When the molecules of the sample are correlated with each other, there is no well defined average state. The observer therefore assigns a probability distribution \( \Pr(\bar{\nu}) \) over the possible values of this “objective element of reality” \( \bar{\nu} \), hence Eq. (3.39).

To put it simply, when macroscopic measurements are coarse with respect to the quantum correlation length scale of the system, they behave classically. Indeed, assume that a sample of \( N \) molecules have quantum correlation length \( \xi \), i.e. there is \( \xi \)-molecule entanglement in the system. Then, all of the above construction can be applied to the \( N/\xi \) collections of \( \xi \) molecules. We simply have to treat each block of entangled \( \xi \) molecules as one big molecule. There is no entanglement between these big molecules so
the previous analysis applies, as long as the measurement accuracy is larger than $\sqrt{\xi/N}$.

Thus, we see that only entanglement on “macroscopic” scales can cause quantum effects to the measurement of coarse grained macroscopic observable.

We have demonstrated in this Section that a classical limit can be obtained for closed quantum quantum system under certain assumptions about the system’s initial state. This approach is complementary to the decoherence program [GJK+96a, Zur03a], where classicality arises from the interaction between the system of interest and its environment. Moreover, the combination of these two approaches extends the conclusions reached in the present Section. When the sample interacts with an environment, it will typically end up in a state that behaves classically under macroscopic measurements. For example, when the effect of this interaction is to dephase or depolarize the molecules of the sample, decoherence will destroy entanglement on macroscopic scales [JB00a], so coarse grained “macroscopic histories” will be consistent. An other possibility is that the environment interacts with the system through a “collective coupling”, i.e. the system observables appearing in the coupling Hamiltonian are of the form Eq. (3.2). This type of interaction will be studied in the next Section. Under such a coupling, the environment is effectively measuring the macroscopic observables appearing in the coupling Hamiltonian. Thus, after the interaction, the system is insensitive to further measurement of the same macroscopic observables. For example, an environment consisting of charged particles interacts with the total magnetization of a ferromagnet, effectively measuring the average value of the Pauli operators $\langle \sigma_x \rangle$, $\langle \sigma_y \rangle$, and $\langle \sigma_z \rangle$ to finite accuracy. Therefore, after decoherence the ferromagnet will not be further disturbed by such measurements.

3.6. NMR information processing

Room temperature nuclear magnetic resonance (NMR) has been for several years a benchmark for quantum information processing [LKC+02a, CLK+00a]. The sample contains $N \approx 10^{20}$ molecules which are to good approximation non-interacting due to dynamical decoupling caused by thermal excitations. Hence, the total Hamiltonian is the sum of the single-molecules Hamiltonians $H = \sum_k h_{(k)}$, it takes the form Eq.(3.2), so it is a macroscopic observable. Initially, the sample is in a thermal state

$$\rho_N = \frac{e^{-\beta H}}{Z} = \frac{e^{-\sum_k h_{(k)}}}{Z} = \left( \frac{e^{-\beta h_z}}{z} \right)^\otimes N$$
where $Z = Tr\{e^{-\beta H}\}$ and $z = Tr\{e^{-\beta h}\}$ are the partition functions of the sample and of a single molecule respectively. Each molecule contains a certain number of nuclei which carry a spin, and it is these spin degrees of freedom that are used to perform the computation. Due to their different chemical environment, the various spins of a molecule can have different Larmor frequencies $\omega_j$, which makes it possible to address them individually. To do so, the sample is placed in a coiled wire through which a sequence of externally controlled radio frequency (RF) current pulses can be applied. By properly tuning the frequency of the RF pulse, we can address all the spins with the same Larmor frequency, so all the $N$ molecules are addressed in parallel. Therefore, a sequence of pulses transforms the state of the sample according to

$$\rho_N \rightarrow U^{\otimes N} \rho_N U^{\otimes N},$$

where $U$ is a unitary matrix acting on the Hilbert space of a single molecule. This transformation preserves the tensor product structure of the density matrix $\rho_N = \nu^{\otimes N}$, it collectively changes the state of individual molecules $\nu$.

It has been known for a long time [BP54a] that the coupling between the nuclear spins and the coil can considerably disturb the state of the sample in certain regimes through back-action. This noise is not fundamentally irreversible, it is only due to our neglecting of high order terms in the coupling Hamiltonian. However, since the coil is also used to read out the state of the sample, it must unavoidably induce extra fundamentally irreversible noise, of the kind discussed in Section 3.3. Indeed, in quantum theory, any measurement that reveals some information must unavoidably perturb the state of the system [BBM92a]. This result is puzzling because the coil is present throughout the computation, not only during the measurement phase, so should in principle disturb the computation.

A simple model to study the effect of this noise was presented in Ref. [LS00b]. The current in the coil can be modeled by a continuous quantum variable $\Phi_j = \int \phi_j |\phi_j\rangle \langle \phi_j|dr_j$ where $j$ labels the modes of the field in the coil. Each field mode $\Phi_j$ couples to the

---

4When the sequence of pulses generates a complex transformation, it is practically impossible to keep track of $\nu$, as this would require an exponential amount of computation. Hence, given our limited computational capacities, the sample should really be described by an exchangeable state of the form Eq.(3.30). Indeed, if we had sufficient computational power to have complete knowledge of the state $\nu^{\otimes N}$ after the pulse sequences, it would mean that the quantum computation was useless since we are able to predict its outcome!
resonant magnetization of the sample — i.e. to the spins of Larmor frequency \( \omega_j \) — through its conjugate momentum \( \Pi_j \). The coupling Hamiltonian takes the form \( H_c = \gamma \sum_j \Pi_j M^x_j \) where \( \gamma \) is some coupling constant (that absorbs the magnetization units \( \frac{1}{\hbar} g \)) and

\[
M^x_j = \sum_{k=1}^N \sigma^x_{j(k)} = N \sum_L (2L - 1)Q^{(N)}_L
\]

is the total transverse magnetization of the \( j \)th specie of nuclei in their rotating frame of Larmor frequency \( \omega_j \). Assume for simplicity that each molecule contain a single spin-\( \frac{1}{2} \) nucleus which couples to the field mode \( \Phi_0 \) (we will thus drop the explicit 0 subscript). This field mode is initially in state \( |\Psi\rangle = \int \Psi(\phi)|\phi\rangle d\phi \) and the sample is in state \( \rho_N \).

After a time \( t \), simple calculations show that the joint state of the field and the sample is

\[
\rho(t) = \sum_{L,L'} \int d\phi d\phi' \Psi(\phi)\Psi^*(\phi')Q^{(N)}_L \rho_N Q^{(N)}_{L'} \otimes |\phi + f(L)\rangle \langle \phi' + f(L')|
\]

where \( f(L) = \gamma t N (2L - 1) \). The field mode \( \Phi_0 \) is subsequently observed to be in state \( |\phi\rangle \), and accordingly the state of the sample is updated to

\[
\rho_N \phi \rightarrow \rho_{N|\phi} = \frac{\text{Tr}_{\text{coil}}\left\{ (|\phi\rangle \langle \phi| \otimes 1) \rho(t) \right\}}{P(\phi)} = \frac{\tilde{Q}^{(N)}_\phi \rho_N \tilde{Q}^{(N)\dagger}_\phi}{P(\phi)}
\]

where \( \tilde{Q}^{(N)}_\phi = \sum_{L'} \Psi(\phi - f(L'))Q^{(N)}_{L'} \) are coarse grained type measurements like those of Eq. (3.11). The initial field configuration \( \Psi(\phi) \) plays the role of the smoothing function, and has width (in the \( L \) domain) \( \sigma \approx \sqrt{\langle \Psi | \Phi_0^2 | \Psi \rangle - \langle \Psi | \Phi_0 | \Psi \rangle^2} / N \gamma t \).

This model may appear overcomplicated, but it is in fact quite simple. The field variable \( \Phi_0 \) — that we can think of as the amplitude of the \( \omega_0 \) Fourier component of the current in the coil — serves as a measurement apparatus: it is by reading the value \( \phi \) of \( \Phi_0 \) that we learn about the magnetization of the spins with Larmor frequency \( \omega_0 \). The coupling Hamiltonian is such that it “shifts” the value of \( \Phi_0 \) by an amount that is proportional to the value of \( M^x_0 \) (the rotating magnetization induces a current in the coil). Thus, determining the amount by which \( \Phi_0 \) got shifted allows us to infer the value of \( M^x_0 \). However, the coil may initially not be in an eigenstate of \( \Phi_0 \), so \( \langle \Psi | \Phi_0^2 | \Psi \rangle - \langle \Psi | \Phi_0 | \Psi \rangle^2 > 0 \) (it will typically be in a coherent state). Thus, our final measure of the value of \( \Phi_0 \) does not allow us to determine exactly by what amount it got shifted: it can only do so up to accuracy \( \sqrt{\langle \Psi | \Phi_0^2 | \Psi \rangle - \langle \Psi | \Phi_0 | \Psi \rangle^2} \), which sets the
accuracy $\sigma$ on the measurement of $M_0^2$. Following the results established in Section 3.3.3, a width $\sigma \gg 1/\sqrt{N} \approx 10^{-10}$ insures us that the measurement does not significantly perturb the computation.

Of course, the measurements achieved in the laboratory are much coarser than $10^{-10}$. Given the results presented in this paper, we could follow [LS00b] and conclude that the presence of the coil (or the NMR measurements in general) induces a negligible disturbance to the state of the sample. However, our analysis does not apply here straightforwardly since NMR measurements are not ideal (see Section 3.2.2). This is because the coil is not in a pure state at room temperature. As a consequence, not only is the coil not in an eigenstate of $\Phi_0$ (such as a coherent state), but it is in a statistical mixture of such states. Consider, for example, the initial state of the coil in a Gaussian mixture of Gaussian-like field modes $\rho_{\text{coil}} \propto \int e^{-\frac{q^2}{2\lambda^2}} |\Psi_q\rangle \langle \Psi_q| dq$ where $|\Psi_q\rangle \propto \int e^{-\frac{(\phi-q)^2}{4\sigma^2}} |\phi\rangle d\phi$ (the $\Psi_q$ are like coherent states centered around the field value $q$). After a coupling time $t$, the observation of the field mode in state $|\phi\rangle$ updates the state of the sample to

$$\rho_N \xrightarrow{\phi} \rho_N|\phi\rangle = \frac{Tr_{\text{coil}} \left\{ (|\phi\rangle \langle \phi| \otimes \mathbb{I}) \rho(t) \right\}}{P(\phi)} = \int e^{-\frac{q^2}{2\lambda^2}} \tilde{Q}^{(N)}_{\phi-q} \rho_N \tilde{Q}^{(N)}_{\phi-q} dq$$

where $\tilde{Q}^{(N)} \propto \sum_{L'} e^{-\frac{(L'-L)^2}{4\sigma^2}} Q^{(N)}_{L'}$. This is the continuous version of the general state update rule Eq.(3.9) for non-ideal measurements. The corresponding POVM elements $E_\phi = \int e^{-\frac{q^2}{2\lambda^2}} \left[ Q^{(N)}_{\phi-q} \right] ^2$ have width $\lambda + \sigma$, which determines the accuracy of the measurement outcomes following Eq.(3.8). However, the Kraus operators $A_{q\Rightarrow} = \tilde{Q}^{(N)}_{\phi-q}$ have width $\sigma$. Following Eq.(3.9), it is this width which governs the disturbance caused to the state. Thus, it is not the measurement coarseness $\lambda + \sigma$ which ultimately determines the disturbance caused to the state, but the details of the measurement process. In this example, the statistical mixture caused by the finite temperature of the coil added an extra source of uncertainty, characterized by the parameter $\lambda$.

It is therefore necessary to have a detailed model of the interaction between the coil and the sample and of the initial state of the coil to evaluate its contribution to decoherence of the state of the molecules. We suspect that, in actual NMR settings, the measurement coarseness is largely due to statistical (thermal) fluctuations of the type of $\lambda$. However, we also suspect the coherent spread of the coil’s wave function $\sigma$ to be much larger than $10^{-10}$, since coherent manipulation of the molecules appears to be
possible despite the coupling to the coil. These questions, however, deserve a separate study.

3.7. Conclusion and open questions

We have demonstrated a tradeoff between macroscopic measurement accuracy and state disturbance for sample of identically prepared quantum systems. A measurement coarseness smaller than \( 1/\sqrt{N} \) causes a disturbance to the state of the system which increases as the size of the ensemble grows, which is in apparent contradiction with the infinite-copy result. However, a measurement coarseness \( \sigma \gg 1/\sqrt{N} \) induces a negligible disturbance to the state of the sample. This demonstrates that coarseness is an essential feature of the macroscopic limit. The type projectors of Eq. (3.4) will unavoidably lead to macroscopic quantum fluctuations regardless of the size of the ensemble. Thus, the classical observables encountered in our everyday life (e.g. position and velocity of a baseball, bulk magnetization of a ferromagnet, etc.) cannot be suitably described in terms of von Neumann macroscopic type projectors Eq. (3.4) — the spectral projectors of average observables Eq. (3.2) — such as prescribed by textbook quantum theory, but require coarse grained POVMs Eq. (3.11). Moreover, as illustrated with the measurement model of Section 3.6, realistic measurements settings give rise to coarse grained POVMs, not projective measure.

Using these results, we have argued that any sequence of macroscopic observations behave essentially classically provided that there is no large-scale entanglement in the sample. More precisely, the measurement of macroscopic observables generate consistent families of histories provided that their coarseness is larger than \( \sqrt{\xi/N} \) where \( \xi \) is the quantum correlation length scale of the system. Under this condition, the quantum state update rule behaves as if the measurements were revealing information about an objective element of reality, namely the average reduced state of a single molecule \( \mathcal{\nu} \). Hence, many independent observers acquiring their information through these measurements will arrive to a common assignment of \( \mathcal{\nu} \). In this operational sense, \( \mathcal{\nu} \) becomes an objective element of reality.

Our analysis does not apply when entanglement becomes present on macroscopic scales. Clearly, not all such entanglement will yield quantum effects on the measurement of macroscopic observables. For example, the “cat state” \( \sqrt{\frac{1}{2}}(|x_1\rangle^\otimes N + |x_2\rangle^\otimes N) \), which is not exchangeable, behaves just like the exchangeable state \( \frac{1}{2}(|x_1\rangle|x_1\rangle)^\otimes N + (|x_2\rangle|x_2\rangle)^\otimes N \)
for all macroscopic observables. Thus, it will be interesting to determine what type of entangled states, if any, will manifest their quantum nature in the measurement of macroscopic observables.

An interesting question arises from the study of the relation between exchangeable states and macroscopic observations. We have seen in Section 3.5 that applying a random permutation to the molecules in a separable state yields a state which is not exchangeable, but possesses similar characteristics. We do not know what type of operation can transform a generic quantum state into an exchangeable one. We suspect that performing a tomographically complete set of macroscopic measurements on subsets of the sample followed by a random permutation of the molecules would do the trick. Physically, this would mean that a collective coupling to the environment and a diffusion process would map any state to an exchangeable state. We also suspect that a random subset of $\sqrt{N}$ molecules out of the $N$ molecules of the sample would also be in an exchangeable state, regardless of the initial state of the sample. This would be very interesting as it would extend the reach of our classicality analysis. Moreover, understanding under what circumstances can a sample of physical systems be treated as if they were all in the same unknown state is of crucial importance since this is assumed in most quantum experiments performed on macroscopic samples (e.g. any type of spectroscopy).

Finally, we have related our study to a NMR measurement model introduced in [LS00b]. We have extended their analysis to the case where the coil is not in a pure mode state but rather in a statistical mixture of such states, like a thermal state. In this case, there are two parameters describing the macroscopic measurements: the width $\sigma + \lambda$ of the POVM elements describes the accuracy of the measurements and width $\sigma$ of the Kraus operators governs the disturbance caused to the state of the sample. Therefore, a measurement accuracy $\sigma + \lambda \gg 1/\sqrt{N}$ does not guaranty a negligible disturbance except when the measurement is ideal. The NMR measurement process therefore deserves a detailed study.
Summary of Chapter 3

- The measurement of a collective property over an ensemble of quantum systems is described by an ordinary von Neumann projective measurement consisting of type projectors.

- Finite accuracy measurement of macroscopic quantities is described by coarse grained POVMs, obtained by “smoothing out” the type projectors.

- The exact measurement of a macroscopic observable greatly disturbs the state of an ensemble of identically prepared quantum systems: the larger the ensemble the greater the disturbance, in apparent contradiction with the infinite ensemble result. In particular, the reduced state of a single molecule of the sample gets completely decohered by macroscopic measurements.

- Measurements of finite accuracy leave the state of an ensemble of identically prepared quantum systems essentially intact, provided that the measurement coarseness is greater than the threshold $1/\sqrt{N}$. The essence of this result is independent of the details of the measurement procedure, as long as it corresponds to an ideal POVM.

- Exchangeable states can be interpreted as if each molecules of the sample were in the same unknown state $\nu$. Macroscopic observables associated with non-commuting observables can be used to “discover” this unknown state $\nu$ without affecting it to high accuracy.

- When there is no entanglement on macroscopic scales across the molecules of the sample, the quantum state update rule applied to the measurement of macroscopic observables will behave as if it were revealing information about an objective element of reality, namely the average reduced state of a single molecule $\overline{\nu}$.

- The coarse grained POVMs we have studied can be constructed with the help of a simple NMR-inspired model. In this case, the measurement accuracy $\sigma$ corresponds to the “coherent spread” of the wave function of the coil. When the coil is in a mixed state, an extra term contributes to the measurement coarseness, so our general state disturbance tradeoff does not apply blindly.
4 — Conclusions

We always have had a great deal of difficulty understanding the world view that quantum mechanics represents. At least I do, because I’m an old enough man that I haven’t got to the point that this stuff is obvious to me. Okay, I still get nervous with it. And therefore some of the young students... you know how it always is, every new idea, it takes a generation or two until it becomes obvious that there’s no real problem. It has not yet become obvious to me that there’s no problem. I cannot define the real problem, therefore I suspect there’s no real problem, but I’m not sure there’s no real problem. [Fey82a]

—RICHARD P. FEYNMAN

If a quantum state were a “physical reality”, then the basic EPR experiment [EPR35a], as described from two different Lorentz frames, would imply that real things do not obey causality. To our taste, this simple argument — let aside all the other compelling arguments, e.g. [CF96a, Per93a, FP00a, Mer01b, CFS02a, Fuc02c, Spe04a] and references therein — necessarily imply that quantum states are not real, they are epistemic.

In fact, there is a classical analogue to this argument. Suppose that two letters, one black and one white, are placed in two sealed envelopes and sent to opposite ends of the earth, where they are received by Gilles and Ray. Both of these observers are informed of the possible contents of the envelopes, but are not told which letter was send to who. At this point, Gilles is asked to describe the content of the envelope in Ray’s possession: “it is a black letter with probability 1/2, or a white letter with probability 1/2” he says. Then, he opens his envelope and discovers that it contains, say, a white letter. Instantaneously, he is asked about Ray’s envelope: “it contains a black letter for sure” is his answer.
Did something mysterious take place? The state assigned to Ray’s envelope went from 50% – 50% to 100% – 0% instantaneously, even though the physical action that triggered this change — the opening of Gilles envelope — took place on opposite faces of the earth! The answer is obvious: Nothing actually “happened” on Ray’s side when Gilles opened his envelope, only Gilles’ knowledge about Ray’s envelope changed.

So what’s so spooky about entanglement? Quantum states, just like probabilities about the content of envelopes, describe our knowledge about physical systems, so it is not surprising that they can change instantaneously when new data are made available to us, even if the system of interest is at a great distance from us. The problem is that there is nothing in quantum theory to play the role of the letters inside the envelopes. This is basically the theorem of John Bell [Bel64a]: the information cannot be about anything local. Since locality and causality are two principles very dear to most physicists, it looks like there is nothing left for this information to describe.

The simplest way out of this awkward position is to simply abandon the idea that this information has to be about something that exists prior to our measurement:

\[ \text{However, there is no logical necessity for a realistic worldview to always be obtainable. If the world is such that we can never identify a reality independent of our experimental activity, then we must be prepared for that, too. [FP00a]} \]

The information represented by a quantum state is only about the outcome of our future intervention into the world, which does not require any \textit{a priori} existence. In the words of Pascual Jordan (quote taken from [Mer85a]) “Observations not only disturb what has to be measured, they produce it.”

Probability theory can be derived as the only sensible way to place a bet in a specific scenario without systematically losing (see [Cav00a] and reference therein). In this sense, probability theory is more a \textit{law of thoughts} than a law of nature; it prescribes the optimal way of reasoning about nature. The analogue role played by the wave function in quantum theory and a probability distribution in classical physics therefore suggest that quantum theory is also a law of thoughts: \textit{quantum theory is the most efficient way of reasoning about the outcome of our future intervention into the world given our past experience}.

In this case, the remaining piece of the puzzle is to explain why most of the time, things seem to exist independently of our intervention: \textbf{we need an interpretation}
for classical physics! This is the achievement of the present dissertation. We have demonstrated that under certain circumstances — that includes precious measurement “clicks”, our aforementioned intervention into the world —, an objective description of the world can emerge from the underlying epistemic quantum description. Thus, if we are willing to abandon the requirement of a physical reality independent of the perception of observers and settle for an operational notion of reality, then, as we have shown in this dissertation, there is nothing wrong with quantum theory, and it is not surprising that we get classical “reality” out of it.

Moreover, the distinction between such an operational notion of objectivity and true objectivity cannot be distinguished by any experiment: our intervention into the world is after all by definition something operational! (It is impossible to prove to someone that everything he perceives is not just a dream. However, demonstrating that under certain circumstances everyone will be having the same dream at the same time is an interesting step in that direction, and is as far as we can go.) We are not saying that this question cannot be settled in the laboratory. For example, some alternatives to quantum theory, such as collapse models [GRW86a], admit objective elements of reality and do lead to different experimental predictions that could in principle be detected. But these are not interpretations of quantum theory, they are different theories altogether (and suffer from other problems of their own...) We do not deny the possibility that some more fundamental theory, that reproduces the predictions of quantum theory in the regimes where it has been tested, might unproblematically admit an objective reality. However, if we accept quantum theory as it is, the answer we have provided here appears (at least to us) to be the only viable one.

To our taste, the only objects that should be of any interest to physical theories are those things that can be, at least in principle, found out by independent observers. As we have demonstrated through a careful study of the mechanisms responsible for our perception of the world, such effectively objective elements do emerge from quantum theory. Under these circumstances, they can play the role of the letters hidden inside the envelopes: the information encapsulated in a quantum state is about the singled-out properties of the world that can be discovered by several independent observers. Thus, if we revisit our notion of reality to this operational standard, “we suspect there is no real problem!”

Of course, like all scientists, we are not entirely satisfied with this state of affairs.
“Anybody who’s not bothered by Bell’s theorem has to have rocks in his head.” [Mer85a]

We would prefer to arrive at the conclusion that there is really something out there, independent of our perception. But effective reality is the best we could achieve from within quantum theory in a world that is local and obeys causality.

Finally, as we have mentioned in the introductory Chapter 1, our program is not committed to the epistemic interpretation of quantum theory that we have followed in this dissertation. Different interpretations of quantum theory clash with classical theories in different ways. Nevertheless, our explanation of the classical is valid as long as the quantum formalism remains intact, and is therefore independent of any interpretation of the theory. This reflects the particularity of our approach: we provide an interpretation to classical theory in terms of the quantum formalism (that we regard as the optimal way of processing our knowledge about nature), not the other way around.
Definition A.0.1 (Trace distance). The trace distance between two density operators $\rho$, $\varrho$ is defined by $D(\rho, \varrho) = \text{Tr} |\rho - \varrho|$. When $\rho$ and $\varrho$ commute, the trace distance is equal to the $L_1$-distance between the classical probability distributions defined by their eigenvalues. Alternatively, the trace distance is equal to $2 \max \rho \text{ Tr } P(\rho - \varrho)$ where the maximum is taken over positive operators $P \leq I$

Definition A.0.2 (Euclidean distance). The Euclidean distance between a pair of density operators $\rho$, $\varrho$ is defined by $\|\rho - \varrho\|_2 = \sqrt{\text{Tr}\{(\rho - \varrho)^2\}}$.

Proposition A.0.1 (Cauchy-Schwartz inequality). $D(\rho, \varrho) \leq \sqrt{d} \|\rho - \varrho\|_2$.

Proposition A.0.2. Let $p_i = \text{Tr}\{A_i \rho\}$ and $q_i = \text{Tr}\{A_i \varrho\}$ be the probabilities of the outcomes of a measurement $\{A_i\}$ for states $\rho$ and $\varrho$ respectively. Then, $D(p, q) \leq D(\rho, \varrho)$.

Proposition A.0.3 (Fanne’s inequality). Let $p_i$ and $q_i$ with $i = 1, 2, \ldots, d$ be two classical probability distributions such that $D(p, q) \leq 1/e$. Then $|H(p) - H(q)| \leq D(p, q) \log d + \eta(D(p, q))$, with $\eta(x) = -x \log x$.

Proposition A.0.4 (Convexity of entropy). Let $P(X_i|Y_j)$ be a set of conditional probability distribution for the random variable $X$, and $P(Y_j)$ be the probability distribution for the random variable $Y$. Then

$$\sum_j \left( - \sum_i P(X_i|Y_j) \ln P(X_i|Y_j) \right) \leq - \sum_i P(X_i) \ln P(X_i) \quad (A.1)$$

where $P(X_i) = \sum_j P(X_i|Y_j)P(Y_j)$.  

97
Proposition A.0.5 (Data processing inequality). Suppose $X \rightarrow Y \rightarrow Z$ is a Markov chain, then $H(X) \geq I(X : Y) \geq I(X : Z)$.

Lemma A.0.1. For any matrix $\rho = \sum_{ij} \alpha_i \alpha_j^* |i\rangle \langle j| \otimes |\Phi^F_i\rangle \langle \Phi^F_j| \gamma_{ij}^F$, with $\alpha_i \neq 0$, and such that,

1. $\langle i| j \rangle = \delta_{ij}$
2. $|\Phi^F_i\rangle$ are linearly independent;
3. $|\gamma_{ij}^F| \leq \gamma^F$ for $i \neq j$, and $\gamma_{ii}^F = 1$ for all $i$;
4. $|\langle \Phi^F_j| \Phi^F_i \rangle| = |\gamma_{ij}^F| \leq \gamma^F$ for $i \neq j$;

there exist a matrix $\varrho = \sum_i |\alpha_i|^2 |i\rangle \langle i| \otimes |\Psi^F_i\rangle \langle \Psi^F_i|$, satisfying

1. $\langle \Psi^F_i| \Psi^F_j \rangle = \delta_{ij}$;
2. $\|\rho - \varrho\|_2 \leq \sqrt{2(d^S - 1)} \gamma^F + \gamma^F + O((\gamma^F)^{3/2} + (\gamma^F)^2)$.

where $d^S$ is the number of non-zero coefficients $\alpha_i$.

Proof The proof of this lemma relies on a careful analysis of Gram-Schmidt orthonormalisation procedure applied to the states $|\Phi^F_i\rangle$.

We define the new set of orthogonal states $|\Psi^F_i\rangle$ by the following equations:

$$|\Psi^F_i\rangle = \frac{1}{N_i} \left( |\Phi^F_i\rangle - \sum_{j<i} |\langle \Phi^F_j| \Psi^F_i \rangle| \langle \Psi^F_j| \Phi^F_i \rangle \right), \quad (A.2)$$

where $N_i$ is a normalization factor.

As a first step, we prove by induction on $i$ that the following properties hold:

$$|\langle \Phi^F_j| \Psi^F_i \rangle| \begin{cases} \leq 2\gamma^F + O((\gamma^F)^2), & j < i \\ \geq 1 - \frac{i-1}{2}(\gamma^F)^2 + O((\gamma^F)^3), & j = i \\ \leq \gamma^F + O((\gamma^F)^2), & j > i \end{cases} \quad (A.3)$$

• $i = 1$. Trivial, since $|\Psi^F_1\rangle = |\Phi^F_1\rangle$.

• $i > 1$. Now, we assume that the Eq. (A.3) holds for $k < i$. By definition of $N_i$ we have,

$$N_i^2 = 1 - \sum_{k<i} |\langle \Phi^F_k| \Psi^F_i \rangle|^2 \geq 1 - (i-1)(\gamma^F)^2 + O((\gamma^F)^3). \quad (A.4)$$
Moreover, with Eq. (A.2) we also have,

$$\left| \langle \Phi F_i | \Psi F_i \rangle \right| = \frac{1}{N_i} \left| \langle \Phi F_j | \Phi F_i \rangle - \sum_{k < i} \langle \Psi F_k | \Phi F_i \rangle \langle \Phi F_j | \Psi F_k \rangle \right|. \quad (A.6)$$

1. When $j < i$ we get

$$\left| \langle \Phi F_j | \Psi F_i \rangle \right| \leq \frac{1}{N_i} \left( \left| \langle \Phi F_j | \Phi F_i \rangle \right| + \left| \sum_{k < i, k \not= j} \langle \Psi F_k | \Phi F_i \rangle \langle \Phi F_j | \Psi F_k \rangle \right| + \left| \langle \Psi F_j | \Phi F_i \rangle \langle \Phi F_j | \Psi F_j \rangle \right| \right) \quad (A.7)$$

$$\leq 2 \gamma F + O((\gamma F)^2). \quad (A.8)$$

2. For $i = j$,

$$\left| \langle \Phi F_i | \Psi F_i \rangle \right| = N_i \geq 1 - \frac{i - 1}{2} (\gamma F)^2 + O((\gamma F)^3). \quad (A.9) \quad (A.10)$$

3. Finally, in the case $j > i$, the contribution at order $\gamma F$ comes from $\langle \Phi F_j | \Phi F_i \rangle$ which gives,

$$\left| \langle \Phi F_j | \Psi F_i \rangle \right| \leq \gamma F + O((\gamma F)^2). \quad (A.11)$$

With this result, we can easily calculate an upper bound on $\| \rho - \varrho \|_2$:

$$\text{Tr} (\rho - \varrho)^2 = \text{Tr} \rho^2 + \text{Tr} \varrho^2 - 2 \text{Tr} \rho \varrho \quad (A.12)$$

$$= 2 \sum_i |\alpha_i|^4 (1 - |\langle \Phi F_i | \Psi F_i \rangle|^2) + \sum_{i \not= j} |\alpha_i|^2 |\alpha_j|^2 |\gamma F_{ij}|^2 \quad (A.13)$$

$$\leq 2(d^S - 1)(\gamma F)^2 + (\gamma F)^2 + O((\gamma F)^3) \quad (A.14)$$

Therefore we have $\| \rho - \varrho \|_2 \leq \sqrt{2(d^S - 1)(\gamma F)^2 + (\gamma F)^2 + O((\gamma F)^3/2)}$, which concludes the proof.

\[ \blacksquare \]
Appendix B — Macroscopic observables: mathematical complement

B.1. Single molecule post-measurement state

We will show how to compute the post-measurement state of a single molecule, namely Eq. (3.24). For this, it will be useful to alter our notation a bit. In this subsection only, we will consider non-normalized types: If \( L(X) \) denotes the normalized type of \( X \), then its non-normalized type is \( N L(X) \). Thus, for this section only, \( L(X) \) is a \( d \)-component vector whose \( j \)th component \( L_j \) equal the number of occurrences of the letter \( x_j \) in \( X \). Adding to the notation, for the type \( L = (L_1, \ldots, L_d) \) of a \( N \)-letter string \( X \), we denote by \( L^{-x_j} = (L_1, \ldots, L_j - 1, \ldots, L_d) \) the type of the string obtained by removing one occurrence of \( x_j \) from \( X \). Of course, this is a well defined type only when \( L_j \geq 1 \).

Given this notation, we can write

\[
Q_L^{(N)} = \sum_j |x_j\rangle \langle x_j| \otimes Q_{L^{-x_j}}^{(N-1)} \tag{B.1}
\]

where the \( Q_{L^{-x_j}}^{(N-1)} = 0 \) when \( L^{-x_j} \) is not a well defined type. Applying the state update rule and tracing out all but a single molecule, we get

\[
\rho_1|L = Tr_{N-1} \left\{ \frac{Q_L^{(N)} \rho_N Q_L^{(N)}}{P(Q_L^{(N)} | \rho_N)} \right\} \\
= \sum_{ij} |x_i\rangle \langle x_i| \nu \langle x_j| Tr \left\{ \frac{Q_{L^{-x_i}}^{(N-1)} \rho \otimes N-1 Q_{L^{-x_j}}^{(N-1)}}{P(Q_L^{(N)} | \rho_N)} \right\} \\
= \sum_j R_j |x_j\rangle \langle x_j| \frac{P(Q_{L^{-x_j}}^{(N-1)} | \rho_{N-1})}{P(Q_L^{(N)} | \rho_N)}; \tag{B.2}
\]

in the last line, we used the definition of the probability Eq. (3.16) and the orthogonality of the type projectors Eq. (3.5). The ratio appearing in the last line can easily be computed as it involves multinomial distributions, it is equal to

\[
\frac{R_1^{L_1} \cdots R_j^{L_j-1} \cdots R_d^{L_d} (L_1, \ldots, L_j-1, \ldots, L_d)}{R_1^{L_1} \cdots R_j^{L_j} \cdots R_d^{L_d} (L_1, \ldots, L_j, \ldots, L_d)} = \frac{1}{N} \frac{L_j}{R_j}.
\]

101
Inserting this in Eq. (B.2) (and keeping in mind the different definitions of \( L_j \)) yields the result Eq. (3.24). Averaging this state over measurement outcomes \( \mathbf{L} \) gives

\[
\rho'_1 = \sum_j R_j |x_j\rangle \langle x_j |. \tag{B.3}
\]

The effect of coarse-grained measurements \( \tilde{Q}_\ell^{(N)} \) on the state of a single molecule can be studied by straightforward modifications of the method outlined above. The results are easily predictable: while the off diagonal elements \( |x_i\rangle \langle x_j| \) of \( \rho'_1 \) are completely suppressed when \( \sigma = 0 \), they only get damped by a factor proportional to \( \text{Tr}\{\tilde{Q}^{(N-1)}_{L-x_i} \rho_{N-1} \tilde{Q}^{(N-1)}_{L-x_j}\} \) with \( \mathbf{L} \approx N \mathbf{R} \) when the measurement is coarse. Since \( \mathbf{L}^{-x_i} \) and \( \mathbf{L}^{-x_j} \) are very close to each other on the probability simplex, this decoherence factor is close to unity when the smoothing function \( q_L(\ell) \) is sufficiently wide.

For example, when we choose a Gaussian smoothing function

\[
q_L(\ell) = \left(\frac{1}{2\pi \sigma^2}\right)^{\frac{d}{2}} \exp\left\{ -\frac{\| \ell - \mathbf{L} \|^2_2}{2\sigma^2 N^2} \right\}
\]

(the extra \( N^2 \) in the denominator of the exponent is due to the special normalization of the types used in this section), elementary algebra can be used to show that the matrix element \( \nu_{ij} \) of the single molecule density matrix \( \nu \) get updated according to

\[
\nu_{ij} \xrightarrow{\ell} \nu_{ij|\ell} = \nu_{ij} \frac{\sum_L q_L(\ell) P(Q^{(N)}_L|\rho_N)L_j/R_j e^{-\ell_j+L_j+\ell_i-L_i+1}}{\sum_L q_L(\ell) P(Q^{(N)}_L|\rho_N)}. \tag{B.4}
\]

The only non-trivial factors in this expression are \( L_j/R_j \) and \( e^{-(\ell_j+L_j+\ell_i-L_i+1)}/N^2\sigma^2 \). However, the probability \( P(Q^{(N)}_L|\rho_N) \) is — according to the typical sequence theorem Eq. (3.1) — very sharply peaked around \( L_j = R_j \), so the factor \( L_j/R_j \) is nearly trivial (i.e. it differs from 1 by \( O(1/N) \)) in dominant terms of the sum. Similarly, the smoothing function \( q_L(\ell) \) becomes very small when \( L_j \) differs from \( \ell_j \) by more than roughly \( N\sigma \). Thus, the argument of the exponential \( e^{-(\ell_j+L_j+\ell_i-L_i+1)}/N^2\sigma^2 \) is of order \( 1/N \) in the dominant terms of the sum, so this factor also differs from unity by \( O(1/N) \). Thus, the disturbance caused to the matrix elements \( \nu_{ij} \) are of relative order \( 1/N \). A more quantitative comparison of the original and final single-molecule state is obtained straightforwardly from our general fidelity tradeoff and the monotonicity of fidelity.
B.2. Conditional fidelity

We will compute, for an ensemble of $N$ molecule initially in state $|\Psi_N\rangle = \sum_{j=1}^{d} \beta_j |x_j\rangle$, the fidelity between the pre- and the conditional post-measurement state $\rho_N$ and $\rho_N|\ell\rangle$ respectively. Starting from Eq. (3.17,3.18), we can express the fidelity

$$F(\rho_N, \rho_N|\ell\rangle) = \langle \Psi_N | \rho_N|\ell\rangle |\Psi_N \rangle$$

$$= \left( \sum_L \sqrt{q_L(\ell)} m(L, R) \right)^2,$$

where $R_j = \langle x_j | \nu | x_j \rangle$, and the multinomial coefficient $m(L, R) = \binom{N}{N_L_1, \ldots, N_L_d} \prod_j R_j^{N_L_j}$.

Assuming that the smoothing function is Gaussian $q_L(\ell) = \left( \frac{1}{2\pi\sigma^2} \right)^{\frac{d}{2}} \exp \left\{ -\frac{\|L - R\|^2}{4\sigma^2} \right\}$, the fidelity takes the form

$$F(\rho_N, \rho_N|\ell\rangle) = \left( \sum_L \exp \left\{ -\frac{\|L - R\|^2}{2\sigma^2} \right\} m(L, R) \right)^2 = \frac{\text{Nom}}{\text{Den}}, \quad (B.5)$$

where $\text{Nom}$ and $\text{Den}$ stand for nominator and denominator respectively.

The lower bound on this expression is found by similar means that lead to the bound on the fidelity between $\rho_N$ and $\rho'_N$ in Section 3.3, except that the presence of a denominator — absent in Eq. (3.25) — creates extra complications. Hence, let’s start by considering the nominator. First, we use the triangle inequality $\|L - R\|_2 \leq \|L - \ell\|_2 + \|R - L\|_2$ to get an upper bound

$$e^{-\frac{\|L - \ell\|^2}{2\sigma^2}} \geq e^{-\frac{(\|L - \ell\|_2 + \|R - L\|_2)^2}{2\sigma^2}}.$$  

Then, just like we did in Section 3.3, we truncate the sum to the domain $\mathcal{D} = \{ L : \|L - R\|_2 \leq \Delta \}$. Clearly on this domain

$$e^{-\frac{\|L - \ell\|^2}{2\sigma^2}} \geq e^{-\frac{(\|L - \ell\|_2 + \Delta)^2}{2\sigma^2}} \quad \text{on } \mathcal{D}. \quad (B.6)$$

Combining these two steps yields

$$\text{Nom} \geq e^{-\frac{(\|L - \ell\|_2 + \Delta)^2}{2\sigma^2}} \left( \sum_{L \in \mathcal{D}} m(L, R) \right)^2$$

$$\geq e^{-\frac{(\|R - |\ell\rangle \|_2 + \Delta)^2}{2\sigma^2}} \left( 1 - e^{-\frac{N \Delta^2}{2}} \right)^2 \quad (B.7)$$
where we appealed to the Cauchy-Schwartz inequality (c.f. Proposition A.0.1) and the typical sequence theorem Eq. (3.1) to get the second line.

Since we are interested in finding a lower bound to the fidelity, we must now find an upper bound to the denominator of Eq. (B.5). To do this, we decompose the sum into 

\[ \sum_{L} = \sum_{L \in D} + \sum_{L \notin D}. \]

The sum outside the domain \( D \) can easily be bounded:

\[
\sum_{L \notin D} e^{-\frac{\|L - \ell\|^2}{2\sigma^2}} m(L, R) \leq \sum_{L \notin D} m(L, R) \leq e^{-\frac{Nd\Delta^2}{2}} \tag{B.8}
\]

where the second line follows from the Cauchy-Schwartz inequality and the typical sequence theorem. For the sum inside \( D \), we use the triangle inequality \( \|L - \ell\|_2 \leq \|L - R\|_2 + \|R - \ell\|_2 \), which translates into

\[ \|L - \ell\|_2 \geq \|\ell - R\|_2 - \Delta \tag{B.9} \]

on the domain \( D \). Before squaring this quantity, it is important to determine whether \( \|\ell - R\|_2 - \Delta \) is a positive or a negative quantity. We shall thus distinguish two cases.

**Case 1:** \( \|\ell - R\|_2 \leq \Delta \). In this case, we use the straightforward bound

\[
\sum_{L \in D} e^{-\frac{\|L - \ell\|^2}{2\sigma^2}} m(L, R) \leq 1.
\]

Combining this with Eq. (B.8) yields \( \text{Den} \leq 1 + e^{-\frac{Nd\Delta^2}{2}} \), so together with the nominator Eq. (B.7), we get a bound on the fidelity

\[
F(\rho_N, \rho_N|\ell) \geq \frac{e^{-\frac{(\|\ell - R\|_2 + \Delta)^2}{2\sigma^2}} \left(1 - e^{-\frac{Nd\Delta^2}{2}}\right)^2}{1 + e^{-\frac{Nd\Delta^2}{2}}} \geq \frac{e^{-\frac{2\Delta^2}{\sigma^2}} \left(1 - e^{-\frac{Nd\Delta^2}{2}}\right)^2}{1 + e^{-\frac{Nd\Delta^2}{2}}} \quad \text{case} \quad \|\ell - R\|_2 \leq \Delta.
\]

**Case 2:** \( \|\ell - R\|_2 > \Delta \). In this case, the inequality Eq. (B.9) gives \( \|L - \ell\|^2 \geq \left(\|\ell - R\|_2 - \Delta\right)^2 \), so the sum on the domain \( D \) is bounded by

\[
\sum_{L \in D} e^{-\frac{\|L - \ell\|^2}{2\sigma^2}} m(L, R) \leq e^{-\frac{(\|\ell - R\|_2 - \Delta)^2}{2\sigma^2}} \sum_{L \in D} m(L, R) \leq e^{-\frac{(\|\ell - R\|_2 - \Delta)^2}{2\sigma^2}},
\]

where we use the typical sequence theorem Eq. (3.1) to get the second line.
so together with Eq. (B.8), we get \( D_{en} \leq e^{-\frac{\|\ell - R\|_2^2 - \Delta^2}{2\sigma^2}} + e^{-\frac{N\sigma^2}{2}} \). Combining this result with the bound on the nominator Eq. (B.7) yields

\[
F(\rho_N, \rho_N|\ell) \geq e^{-\frac{\|\ell - R\|_2^2 + \Delta^2}{2\sigma^2}} \left( 1 - e^{-\frac{N\Delta^2}{2}} \right)^2 \frac{1 + e^{-\frac{N\sigma^2}{2} + \frac{\|\ell - R\|_2^2 + \Delta^2}{2\sigma^2}}}{1 + e^{-\frac{N\sigma^2}{2} + \frac{\|R - \ell\|_2^2 - \Delta^2}{2\sigma^2}}},
\]

or using the fact that the \( L_2 \)-distance is bounded by \( \| p - q \|_2 \leq 2 \) for any two probability distributions \( p \) and \( q \),

\[
F(\rho_N, \rho_N|\ell) \geq e^{-\frac{2\Delta}{\sigma^2}} \left( 1 - e^{-\frac{N\sigma^2}{2}} \right)^2 \frac{1}{1 + e^{-\frac{N\sigma^2}{2} + \frac{\|\ell - R\|_2^2 + \Delta^2}{2\sigma^2}}}, \quad \text{case } \| \ell - R \|_2 > \Delta. \quad (B.10)
\]

This second case gives the worst bound, so Eq. (B.10) turns out to be universal, independent of the sign of \( \|\ell - R\|_2 - \Delta \). The cutoff \( \Delta \) is a free parameter, so we should again try to optimize it in order to achieve the tightest bound. We have not found a closed form expression for this optimum. However, any assignment \( \sigma = N^{-a} \) and \( \Delta = N^b \) with \( 2b < 1 \), \( 2a < b \), and \( 2a < 1 - 2b \) yields

\[
F(\rho_N, \rho_N|\ell) \geq \frac{e^{-AN^{-\alpha}} \left( 1 - e^{-BN^\beta} \right)^2}{1 + e^{-CN^\gamma}} \approx 1 - \frac{A}{N^\gamma} - 2e^{-BN^\beta} - e^{-CN^\gamma}
\]

for some positive constants \( A, B, C, \alpha, \beta, \) and \( \gamma \). For example, when the accuracy of the measurement apparatus is fixed to a constant \( \sigma \), setting the arbitrary cutoff parameter \( \Delta = N^{-1/3} \) gives

\[
F(\rho_N, \rho_N|\ell) \gtrsim 1 - \frac{2}{\sigma^2 N^{1/3}} - 3e^{-\frac{N^{1/3}}{2}}
\]

to first order.
Appendix C — Other work published during Ph.D. program

C.1. Robust polarization-based quantum key distribution over collective-noise channel†

Jean-Christian Boileau\textsuperscript{1}, Daniel Gottesman\textsuperscript{2}, Raymond Laflamme\textsuperscript{1,2}, David Poulin\textsuperscript{1,2}, and Robert W. Spekkens\textsuperscript{2}

\textsuperscript{1}Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada.
\textsuperscript{2}Perimeter Institute for Theoretical Physics, 35 King Street N., Waterloo, ON, N2J 2W9, Canada.

\textbf{Abstract:} We present two polarization-based protocols for quantum key distribution. The protocols encode key bits in noiseless subspaces or subsystems, and so can function over a quantum channel subjected to an arbitrary degree of collective noise, as occurs, for instance, due to rotation of polarizations in an optical fiber. These protocols can be implemented using only entangled photon-pair sources, single-photon rotations, and single-photon detectors. Thus, our proposals offer practical and realistic alternatives to existing schemes for quantum key distribution over optical fibers without resorting to interferometry or two-way quantum communication, thereby circumventing, respectively, the need for high precision timing and the threat of Trojan horse attacks.

Quantum key distribution (QKD), such as the BB84 protocol proposed by Bennett and Brassard in 1984, allows two parties (Alice and Bob) to generate an arbitrarily long random secret key provided that they initially share a short secret key and that they have access to a quantum channel [BB84a]. As opposed to classical key distribution, the secrecy of the generated key does not rely on computational assumptions but simply on the laws of physics: as long as quantum mechanics holds, the information available to an eavesdropper (Eve) can be made arbitrarily small.

Photons are obvious candidates for mediators of quantum information since they are fast, cheap, and interact weakly with the environment. Both free air and optical fiber based QKD have been realized experimentally; see [GRT+02a] and [HND+02a] for reviews. Any experimental implementation of QKD naturally has to deal with the issue of noise in the quantum channel, which substantially complicates the security of QKD, as Eve may attempt to disguise her eavesdropping attempt as noise from another source. Standard security proofs deal with channel noise, including photon loss, and show that Eve acquires essentially no information provided the noise rate is not too high. Higher noise rates mandate lower key generation rates, and once the noise becomes too large, secure key generation is impossible.

Building a viable quantum cryptographic system therefore depends on ensuring that the noise rate is low. The degree of freedom used to encode the information can be the polarization of the photon, its phase, or some combination of both. Purely phase-based schemes have been realized experimentally [TRT93a] but require complex interferometric setups, high precision timing, and stable low temperatures.  

For the sake of practicality, most schemes now incorporate photon polarization as a building block, but these also come with their disadvantages. Optical fibers rotate polarizations of transmitted photons, and the degree of rotation fluctuates over time. If left untreated, this would result in an unacceptably high error rate. A number of proposals have been made to handle this source of errors; we present a new solution which is in some ways superior. Singlet states of two photons have the property that

---

1Interferometry becomes even more challenging with multi-photon states because of the difficulty of keeping phase coherence between the photons. Even with an optimistic estimate of the accuracy with which a particular photon wavelength can be prepared experimentally, namely $10^{-5} \text{nm}$ for wavelengths on the order of micrometers, the phase coherence can only persist for 100m. A scheme which escapes some of these limitations was proposed recently [WAS+03a].
they are unchanged under equal rotations on both qubits. We present two protocols that take advantage of this property to encode key bits in four- or three-photon states. These states should be experimentally realizable, and form simple examples of a noiseless subspace or subsystem, respectively (also called a decoherence-free subspace and decoherence-free subsystem) [ZR97c, KLV00a, KBLW01a].

Free-space QKD is largely immune to the problem of polarization rotation: the coupling between the photons and the molecules in the atmosphere can be absorbed in a dielectric constant to very good approximation. The same unfortunately cannot be said about optical fiber. Rather, the dielectric constant acquires a spatial and temporal dependence, yielding an overall time dependent unitary transformation of the polarization state of a single photon, \( U(t) \), as the net effect of the fiber. This varies on the time-scale of thermal and mechanical fluctuations of the fiber, the shortest of which we will refer to as \( \tau_{fluc} \). If the time delay between the photons is small compared to \( \tau_{fluc} \), the effect of this noise on the state of \( N \) photons is well approximated by

\[
\rho_N \rightarrow [U(t)]^\otimes N \rho_N [U(t)^\dagger]^\otimes N, \tag{C.1}
\]

where \( t \) now denotes the time of transmission. This is known as the unitary collective noise model [ZR97c].

There are several ways to deal with collective noise. The most obvious way is to continuously estimate the transformation \( U(t) \) and systematically compensate for it. However, this requires an interruption of the transmission and, if the fluctuations become too rapid, the communication channel becomes useless. A second possibility — a phase-polarization hybrid which has been used successfully to realize QKD over 67km [SGG+02a] — uses the Faraday orthoconjugation effect [Mar89a] to autocompensate the effect of \( U(t) \). Roughly speaking, if the transformation on the photon during its transmission from Bob to Alice is described by \( U(t) \), it can be \( U(t)^{-1} \) when the photon is transmitted back from Alice to Bob, yielding no net transformation overall. The quantum information can be encoded by an extra phase transformation performed by Alice before returning the photon to Bob. Obviously, this technique only works if \( U(t) \) is roughly constant throughout the transmission of the photon; this sets an upper limit of \( c\tau_{fluc} \) to the distance over which QKD can be implemented with this scheme.\(^2\)

\(^2\)However, with today’s technology, photon loss is a much more serious limitation to the distance over which QKD can be achieved.
Although such two-way quantum communication can eliminate collective noise, it allows for new attacks not possible against BB84. Since Alice receives and emits signals, it is possible for Eve to probe her laboratory — a technique known as the Trojan horse attack.\(^3\) There are many ways in which she can do this. She could add a weak signal to the channel at a slightly different frequency and recover some information about Alice’s phase transformation by subsequently filtering the output signal. Eve could also try to entangle an ancilla system with the signal before it enters Alice’s lab and perform a joint measurement on the two after Alice has retransmitted the signal. She could also intercept the signal and send a different signal to Alice, and thereafter measure the output to estimate the applied phase transformation, etc. Technical solutions for some of these attacks have been proposed. However, Eve has an enormous variety of attacks available, and to prove true information-theoretic security, one must assume that Eve has arbitrary technological power; for instance, she can outperform the best frequency filtering available to Alice and Bob. Because of its inherent use of two-way quantum communication, the protocol is formally quite different from the standard BB84 protocol, and proving its security may be quite difficult.\(^4\)

The schemes we propose here are purely polarization-based and cope with collective noise without resorting to two-way quantum communication. In the first protocol, the quantum information is encoded in a noiseless subspace, while in the second protocol, it is encoded on a noiseless subsystem. A noiseless subspace is invariant under the action of the collective noise operation (here \(U^{\otimes N}\)). Any state within it is therefore unaffected (modulo a global unphysical phase) by the noise. When such a subspace does not exist, it may still be possible to find a set of density operators which are invariant under the effect of noise. These density operators instead form a noiseless subsystem on which pure states can be encoded.

As a simple example, for 2 qubits one has a four-dimensional Hilbert space, with a one-dimensional noiseless subspace corresponding to the singlet state \(|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\), where \(|0\rangle, |1\rangle\} is any basis of the qubit Hilbert space. (If one’s qubits are the

\(^3\)Here, we use “Trojan horse” to refer only to those attacks taking advantage of the inherent input-output on Alice’s end of the channel; they do not apply to the original BB84 scheme.

\(^4\)Note, however, that QKD must make use of two-way classical communication between Alice and Bob, and this presents no particular barrier to security proofs. Indeed, taking full advantage of two-way classical communication results in a protocol with substantially greater tolerance for noise [GL03a].
polarizations degrees of freedom of single photons, as we assume here, then $|0\rangle$ and $|1\rangle$ can be taken to denote, for instance, the vertical and horizontal polarization states.) As is well-known, the singlet state is invariant under equal rotations of both photons; this is precisely the defining property of a noiseless subspace.

The protocols we present use singlet states as building blocks. Information is encoded in the pairing of the photons; the various ways of organizing three or more photons into pairs provide us with different states with which to encode information. It is therefore crucial that information about the pairing resides only in the polarization state of the photon. For example, variations in the frequency of the photons can reveal pairing information: the frequencies of the two photons in each singlet must add up to the frequency of the pump, but the frequencies of photons in different singlets need not match. By measuring the energy of the photons, but not their polarization, Eve can learn about how they are paired without affecting the outcomes of Bob’s measurements. This energy signature of the pairing can be eliminated by filtering the photons before they leave Alice’s lab. Indeed, if the band-width of the filter is smaller than the band-width of the laser, almost no information about the pairing can be recovered by Eve. Similarly, we must wash out the phase relation between photon pairs.

The photons must be distinguishable if different pairings are to correspond to different physical states: they need to be labelled in some way. Physically, this means that the photons must differ with respect to some degree of freedom. Here, the photons are assumed to differ in their time of arrival; they are spatially separated in the optical fiber. Furthermore, each bit is encoded on multi-photon states which must also be distinguished even in the presence of noise. Therefore, the multiplets of photons must be spatially separated by a distance greater than the separation between individual photons inside a multiplet. The fluctuation time $\tau_{\text{fluc}}$ needs only to be large with respect to the difference in the arrival times of the first and last photon of a multiplet.

We will now present our two protocols: the first one encodes the quantum information on four-photon states while the second only requires three-photon states. We do not prove their security here, but rather point only to their similarities with a protocol proposed by Bennett in 1992 (B92) [Ben92a] which is known to be secure [TKI02a]. We hope to provide a complete security proof in a later paper. The first protocol requires
the definition of three normalized states of a photon quartet:

\[ |\psi_1\rangle = \frac{1}{\sqrt{2}} (|a\rangle - |b\rangle) \]
\[ |\psi_2\rangle = \frac{1}{\sqrt{2}} (|c\rangle - |b\rangle) \]
\[ |\psi_3\rangle = \frac{1}{\sqrt{2}} (|a\rangle - |c\rangle) \]  

(C.2)

All these states correspond to pairs of singlet states: in \(|\psi_1\rangle\), photons one and two form a singlet state and so do photons three and four. The two other states correspond to the two other possible ways of pairing four photons as is illustrated by the diagrams. The states are invariant under uniform rotations, so in any basis, these states can be decomposed into the superpositions noted above, where

\[ |a\rangle = \frac{1}{\sqrt{2}} (|0110\rangle + |1010\rangle) \]
\[ |b\rangle = \frac{1}{\sqrt{2}} (|0101\rangle + |1001\rangle) \]
\[ |c\rangle = \frac{1}{\sqrt{2}} (|0011\rangle + |1100\rangle) \]

It is straightforward to verify that \(|\langle \psi_i | \psi_j \rangle| = 1/2 \) for \( i \neq j \). It is therefore impossible to reliably distinguish any pair of these states, but it is possible to make a measurement that provides some information. Measuring the polarization of all four photons allows Bob to distinguish the states \(|a\rangle\), \(|b\rangle\), and \(|c\rangle\). Therefore, if Alice restricts her transmission to one of a pair of states, Bob can tell which of the two states she sent 50% of the time. For example, suppose Alice transmits one of the pair \(|\psi_1, \psi_2\rangle\). When Bob measures either “0101” or “1010”, he can conclude that she sent \(|\psi_1\rangle\). When he gets either “1100” or “0011”, he concludes she sent \(|\psi_2\rangle\). Given any other outcome, Bob can not deduce with certainty which state she sent. We now present the protocol.

**Protocol 1**

1. Alice chooses a random \((4 + \delta)n\) bit string \(X\) and a random \((4 + \delta)n\) trit string \(B\).
2. Alice encodes each bit \(\{0, 1\}\) of \(X\) according to \(\{\psi_1, \psi_2\}\) if the corresponding trit of \(B\) is 0; \(\{\psi_2, \psi_3\}\) if \(B\) is 1; or \(\{\psi_3, \psi_1\}\) if \(B\) is 2.
3. Alice sends the \((4 + \delta)n\) quartets of photons to Bob.
4. Bob receives the photons, and announces this fact. For each of the \((4 + \delta)n\) photon quartets, he randomly chooses between the rectilinear or diagonal polarization.
C.1. Robust polarization-based quantum key distribution over collective-noise channel

basis. He then measures each of the four photons of each quartet according to this choice of basis.

5. Alice announces $B$. Bob can now determine the value of some of the bits of $X$ using the procedure described above.

6. Alice and Bob discard all bits where Bob’s measurement was inconclusive given Alice’s preparation. With high probability, there are at least $2n$ bits left which they keep. Otherwise, they abort the protocol.

7. Alice selects a random subset of $n$ bits and tells Bob which bits were selected.

8. Alice and Bob announce and compare the value of the $n$ selected bits to estimate Eve’s interference; if more than an acceptable number of errors are found, they abort the protocol.

9. Alice and Bob perform information reconciliation and privacy amplification on the remaining $n$ bits.

In step 4, the choice of basis does not affect the measurement outcome of Bob: this is in fact the main property of the encoding. Nevertheless, it is crucial that Eve does not know in which basis the measurement is performed. If she knew, she could measure in the same basis as Bob, and would know everything Bob knew. Since she does not know, she will frequently measure in a different basis than Bob and therefore introduce errors that will reveal her presence.

As the protocol is written, in step 6, Alice and Bob discard any bits for which Bob’s measurement is inconclusive. Nevertheless, an inconclusive result could still be useful. Indeed, any measurement result whose weight differs from 2, e.g. “1011”, indicates that Eve has tampered with the communication. This provides Alice and Bob with some extra data to estimate Eve’s interference: only allowed code-words should be observed by Bob.

If steps 4 and 5 are inverted — which could only provide Eve with more information — we get a protocol quite similar to B92. Alice encodes the bit in two preselected nonorthogonal states which she sends down the quantum channel. Bob then performs a von Neumann measurement chosen at random from a certain set, which can be cast in terms of a positive operator valued measurement (POVM): this is also required in B92.
Nevertheless, there are certain differences in the nature of these POVMs which must be studied carefully to arrive at a complete security proof. We are currently working on these issues. The B92 protocol is not secure if the transmission rate is below 1/2. Indeed, Eve can replace the noisy channel by a perfect channel and measure Alice’s output: with probability 1/2, she gets a conclusive result, in which case she sends the known state to Bob; in the case of an inconclusive result, she does not send anything. From Alice and Bob’s point of view, this would be indistinguishable from the natural noise. By delaying the announcement of $B$, our proposal escapes this limitation.

The simplicity of the measurement single photon polarization is a clear advantage of this protocol. (The possibility of discriminating between states that are invariant under collective noise, without having recourse to collective measurements, has also been noted in Ref. [Cab03a].) Furthermore, proof of principle for photon based noiseless subspace has been realized [KBAW00a] and the specific states required by our protocols have already been produced by several groups [PDG+01a, ZYC+03a]. Two singlet states can be produced in a short time interval via parametric down-conversion by sending a femtosecond pump laser pulse back and forth across a crystal (using a mirror). Since the photons are emitted in different directions, the EPR pairs can be clearly distinguished. The achieved production rate are relative low (a few hertz), but this technique is still in its infancy. Optical delays and switches can be used to create any of the three states of Eq. C.2.

At first glance, it looks like there are two copies of the information in this encoding. For instance, if $B = 0$, so Alice sends either $|\psi_1\rangle$ or $|\psi_2\rangle$, the value of the first two measurement outcomes is enough to deduce the value of the encoded bit: $X = 0$ if the outcome are the same and $X = 1$ otherwise. The same holds for the measurement outcomes on the last two photons. Nevertheless, this redundancy is intrinsic to our quantum encoding scheme and doesn’t provide Eve with any extra information. The second protocol we present exploits this redundancy to reduce the size of the encoding.

Protocol 2 is a slight modification of Protocol 1. In step 3, instead of sending the entire state to Bob, Alice randomly discards one photon from each quartet and sends the remaining three. In step 5, Alice should also announce which photon she has discarded.
Therefore, the three pure states of Eq. C.2 are replaced by the three mixed states

\[
\rho_1 = \begin{pmatrix} 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 \end{pmatrix}, \quad \rho_3 = \begin{pmatrix} 1 \end{pmatrix}
\]

where the "\(\circ\)" denotes the maximally mixed state. These states are obviously invariant under collective noise. Furthermore, any pair can be distinguished with a finite probability, just as with the states in Protocol 1. This follows from the fact that they constitute non-orthogonal mixed states with non-identical supports, and the fact that one can achieve probabilistic error-free discrimination of such mixed states [RST03a]. For example, suppose that Alice has announced that the bit is encoded as \(\{\rho_1, \rho_2\}\).

Clearly, any measurement outcome of Bob’s where photon 1 and photon 2 come out parallel rules out the state \(\rho_1\). Here, the two outcomes “000” and “111” never occur in the absence of eavesdropping; they indicate that Eve has tampered with the communication.

These states do not form noiseless subspaces, because any particular pure state in the decomposition of the density matrices \(\rho_1, \rho_2, \text{ or } \rho_3\) does not remain invariant under collective noise. Instead it is transformed into another state in the decomposition of the same density matrix. For instance, \(|\Psi^-\rangle \otimes |0\rangle\), in the decomposition of \(\rho_1\), becomes under collective bit-flip \(|\Psi^-\rangle \otimes |1\rangle\). The individual states are not noiseless, but the space spanned by them is; therefore they form a noiseless subsystem, and the density matrices are invariant under collective noise.

This second protocol shares many similarities with Protocol 1. It is our hope that essentially the same proof will be able to show both protocols are secure. In practice, Alice does not have to create two photon pairs and discard one photon; she could simply create one pair and one additional photon in the maximally mixed state. This should greatly increase the optimal transmission rate since pair creation schemes have relatively low efficiency. Furthermore, Protocol 2 — based on trios of photons instead of quartets — should suffer less from photon loss and hence be realizable over greater distances.

On a speculative tone, perhaps the two protocols could be hybridized into a more robust protocol. Alice could always encode her information on photon quartets. Bob could then divide the photon multiplets into two sets depending on how many photons from the quartet actually made it to the destination: set 1 when all four photons made
it and set 2 when only 3 photons were detected. The outputs from set 1 could then be used to complete Protocol 1 while those of the second set would be used as in Protocol 2. However, this suggestion provides Eve with a wide variety of attacks unavailable in our two protocols, and its security must therefore be studied on a different basis.

We thank Gilles Brassard for helpful comments on our protocols. J.-C.B., D.P., and R.W.S. receive financial support from Canada’s NSERC.
C.2. Exponential speed-up with a single bit of quantum information: Measuring the average fidelity decay†

David Poulin\textsuperscript{1,2}, Robin Blume-Kohout\textsuperscript{3}, Raymond Laflamme\textsuperscript{1,2}, and Harold Ollivier\textsuperscript{4}

\textsuperscript{1}Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada.
\textsuperscript{2}Perimeter Institute for Theoretical Physics, 35 King Street N., Waterloo, ON, N2J 2W9, Canada.
\textsuperscript{3}Theoretical Division, LANL, MS-B213, Los Alamos, NM 87545, USA.
\textsuperscript{4}INRIA - Projet Codes, BP 105, F-78153 Le Chesnay, France.

**Abstract:** We present an efficient quantum algorithm to measure the average fidelity decay of a quantum map under perturbation using a single bit of quantum information. Our algorithm scales only as the complexity of the map under investigation, so for those maps admitting an efficient gate decomposition, it provides an exponential speed up over known classical procedures. Fidelity decay is important in the study of complex dynamical systems, where it is conjectured to be a signature of eigenvector statistics. Our result also illustrates the role of chaos in the process of decoherence.

A physical experiment consists in evolving a system from its initial state and performing a measurement. It is by now well appreciated that quantum computers can be used to simulate the evolution of certain quantum systems efficiently \cite{Llo96a,Zal98b}. The time evolution operator $U(t',t)$ of a $N$-dimensional quantum system can always be approximated by a product of elementary “gates” of a $K \approx \log_2 N$-qubit quantum computer. Moreover, for a wide class of Hamiltonians, the number of gates $L$ required in this decomposition grows only polynomially with $K$ and $|t'-t|$: such a simulation is called efficient. This is in contrast with classical simulations which typically require computation time growing as the dimension of the Hilbert space of the system, i.e. exponentially with $K$. However, evolution is only one ingredient of a physical experiment. A quantum simulation should also incorporate state initialization and readout, which are generally non trivial, e.g. there are indications that preparing the ground state of a generic Hamiltonian requires an exponential number of gates \cite{vDMV01a}. In this Letter, we present a quantum circuit to evaluate a dynamical quantity, namely the average fidelity decay, which circumvents the need to prepare a complex initial state, requires a very simple measurements, and uses a single bit of quantum information.

Fidelity decay (FD) was initially proposed as a signature of quantum chaos by Peres \cite{Per84a}, and has since been extensively investigated \cite{JP01a,CLM+01a,BC02a,PZ02a,JSB01a}. It measures the rate at which identical initial states diverge when subjected to slightly different dynamics. The discrete time evolution of a closed quantum system can be specified by a unitary operator $U$, where $\rho(\tau_n) = U^n \rho_0 (U^\dagger)^n$. To examine FD, we construct a slightly perturbed map $U_p$, where $U_p = UP$ with $P = \exp\{-i\delta V\}$ for some small $\delta$ and a hermitian matrix $V$. It is conjectured that the overlap (or fidelity)

$$F_n(\psi) = \left| \langle \psi | (U^n)^\dagger U_p^n | \psi \rangle \right|^2$$

(C.4)

between initially identical states $\psi$ undergoing slightly different evolutions, $U$ and $U_p$, should decay differently (as a function of the discrete time $n$) for regular and chaotic dynamics. While the behavior of these decay rates is not fully understood, some of its general features are now widely accepted. In particular, chaotic maps exhibit a universal response to perturbations: the decay rate is governed only by the strength $|V^2|\delta^2$ of the perturbation. This is because FD is an indicator of the relative randomness of the perturbation $V$ in the eigenbasis of the quantum map $U$ \cite{EWL+02a}. On the other hand, the decay rate of regular system depends on details of $V$, so in particular it can
be much slower under simple perturbations. Hence, FD provides a powerful diagnostic of chaotic behavior, but calculating it is computationally hard classically. Furthermore, because $F_n(\psi)$ generally shows large fluctuations over time, it is in practice necessary to average $F_n(\psi)$ over a random set of initial states $\psi$ to determine its decay rate, thus increasing the numerical burden.

Since fully controllable and scalable quantum computers are still quite a ways in the future, algorithms which can be performed on a less-ambitious quantum information processor (QIP) are of great interest. A QIP is a quantum device which may fail to satisfy one or more of DiVincenzo’s five criteria, but can nonetheless carry out interesting computations [BKC+02a]. Of particular interest to us is deterministic quantum computation with a single bit (DQC1) [KL98b], a model of quantum information processing which is believed to be less powerful than universal quantum computation and which is naturally implemented by a high temperature NMR QIP [CLK+00a]. In this model, universal control over all qubits is still assumed, but state preparation and read-out are limited. The initial state of the $(K + 1)$-qubit register is

$$\left(\frac{1 - \gamma}{2} \mathbb{I} + \gamma |0\rangle \langle 0|\right) \otimes \frac{\mathbb{I}}{2^K},$$  \hspace{1cm} (C.5)

i.e., the first qubit (called the probe qubit for reasons which will become clear) is in a pseudo-pure state, whereas the other $K$ qubits are in the maximally mixed state. Furthermore, the result of the computation is obtained as the noisy expectation value of $\sigma_z$ on the probe qubit. The variance of $\sigma_z$ is determined by $i$) the polarization $\gamma$ of Eq. C.5 and $ii$) the “inherent noise” of the measuring process. The value of $\gamma$ in high-temperature NMR is independent of the size of the register because only a single qubit needs to be in a pseudo-pure state. The inherent noise receives contribution from both electronic noise and statistical fluctuations due to the finite sample size. Hence, $\langle \sigma_z \rangle$ can be estimated to within arbitrary $\epsilon$ with a probability of error at most $p$ by repeating the computation $O(\log(1/p)/\epsilon^2)$ times [Hub81a].

Efficient gate decomposition of some quantized chaotic systems have been known for some time [Sch98b, GS01a, BCMS01a], and have recently been incorporated into efficient quantum simulations [ELP+04a, EWL+02a, PLMP03a]. In Ref. [ELP+04a], an efficient quantum circuit is constructed to evaluate the coarse grained local density of states — the average profile of the eigenstates of $U$ over the eigenbasis of $U_p$ — which is believed to be a valid indicator of chaos and is formally related to FD via Fourier
transform [JSB01a]. In Ref. [EWL+02a], an efficient procedure to estimate the FD using the standard model of quantum computation is presented. Finally, in Ref. [PLMP03a], a DQC1 circuit is presented to estimate the form factors $t_n = |\text{Tr}(U^n)|^2$ of a unitary map $U$ which, under the random matrix conjecture (see [Haa01a] and refs. therein), is a good signature of quantum chaos. The proposed algorithm offers only a quadratic speedup, but since entanglement is very limited in DQC1 [ZHS98a, BCJ+99a], this result raises doubt about the common belief that massive entanglement is responsible for quantum computational speed-up [EJ98a, Joz98b].

Drawing upon this previous work, we will now construct an efficient DQC1 algorithm to evaluate the average FD associated with any pair of unitary operators $U$ and $U_p$, provided they can be implemented efficiently, e.g. as those of Refs. [Sch98b, GS01a, BCMS01a]. We begin by proving a crucial identity required to implement the efficient algorithm.

Let $f(\psi)$ be a complex-valued function on the space of pure state of a $N$-dimensional quantum system. We denote its average by $\bar{f}(\psi) = \int f(\psi) d\psi$, where $d\psi$ is the uniform measure induced by the Haar measure, such that $\int d\psi = 1$. For sake of compactness let $\langle \psi | A | \psi \rangle = \langle A \rangle $.\psi.

**Theorem:** Let $A, B, C, \ldots$ be $\ell$ linear operators on a $N$-dimensional Hilbert space. Then

$$
\langle A \rangle \langle B \rangle \langle C \rangle \ldots = \frac{\text{Tr}\left\{ (A \otimes B \otimes C \ldots) P_S^{(\ell)} \right\}}{(N+\ell-1)} \quad (C.6)
$$

where $P_S^{(\ell)}$ is the projector on the symmetric subspace of $\ell$ systems, see Ref. [BBD+97a] for details on $P_S^{(\ell)}$.

**Proof:** First, note that

$$
\langle A \rangle \langle B \rangle \langle C \rangle \ldots = \text{Tr}\left\{ |\psi\rangle \langle \psi|^{\otimes \ell} (A \otimes B \otimes C \ldots) \right\}.
$$

Therefore, the average over the pure states $\psi$ yields,

$$
\text{Tr}\left\{ |\psi\rangle \langle \psi|^{\otimes \ell} (A \otimes B \otimes C \ldots) \right\}.
$$

Since $|\psi\rangle \langle \psi|^{\otimes \ell}$ annihilates any state which is antisymmetric under interchange of two of the $\ell$ systems, and is by construction symmetric under such interchange, it must be proportional to the projector $P_S^{(\ell)}$ onto the symmetric subspace. To establish the theorem it is sufficient to find the proportionality factor $\lambda$ between these two quantities.
Letting $A = B = C = \ldots = I$, we get $1 = \text{Tr}\{|\psi\rangle\langle\psi|^\otimes\ell\} = \lambda \text{Tr}\{P_\ell^{(\ell)}\} = \lambda^\ell (N^\ell - 1)$ (see Ref. [BBD+97a]), which completes the proof. □

A useful corollary to this Theorem for any specific $\ell$ can be obtained by expanding $P_\ell^{(\ell)}$ in Eq. C.6. In the case $\ell = 2$, it reads

$$\langle A \rangle_\psi \langle B \rangle_\psi = \sum_{ijmn} \frac{2A_{ij}B_{mn}(P_2^{(2)})_{ji, nm}}{N^2 + N}$$

$$= \sum_{ijmn} \frac{A_{ij}B_{mn}(\delta_{ij}\delta_{mn} + \delta_{im}\delta_{mj})}{N^2 + N}$$

$$= \frac{\text{Tr}\{A\} \text{Tr}\{B\} + \text{Tr}\{AB\}}{N^2 + N}.$$  \hfill (C.7)

Similar expressions can be derived for $\ell > 2$, which involves the properly normalized sum of all combinations of traces of products and products of traces.

**Efficient algorithm**

To arrive at our algorithm, it is sufficient to write the average fidelity as $F_n(\psi) = \langle (U^n)\dag U^n_p \rangle_\psi \langle (U^n)\dag U^n_p \rangle_\psi$, and apply the identity from Eq. C.7 to obtain

$$F_n(\psi) = \left| \frac{\text{Tr}\{(U^n)\dag U^n_p\}}{N^2 + N} \right|^2 + N.$$  \hfill (C.8)

The specific form of our theorem with $\ell = 2$, unitary $A$, and $B = A\dag$ was discovered by M., P., and R. Horodecki [HHH99b], but our proof simplifies the presentation. An efficient DQC1 algorithm to evaluate the trace of any unitary operator [here, $(U^n)\dag U^n_p$], provided that it admits an efficient gate decomposition, was presented in Ref. [MPS+02a]. If the perturbed map takes the form $U_p = UP$ for some unitary operator $P$ (e.g., $P = \exp\{-i\delta V\}$ as above), the circuit can be further simplified into the one illustrated on Fig. C.1.

We now analyze the complexity of our algorithm. We assume that $U$ and $U_p$ admit $\epsilon$-accurate gate decompositions whose sizes grow as $L(K, \epsilon) \in \text{poly}(K, 1/\epsilon)$. This implies that the controlled version of these gates also scale as $L(K, \epsilon)$ [BBC+95a]. We see from Eq. C.8 that the variance of $F_n(\psi)$ is at most twice the variance of $\text{Tr}\{(U^n)\dag U^n_p\}/N$. Therefore, the overall algorithm – estimating $F_n(\psi)$, to within $\epsilon$, with error probability at most $p$ – requires resources growing as $L(K, \epsilon)n \log(1/p)/\epsilon^2$, so it is efficient. (The range in $n$ over which the decay is studied should be independent of the system’s size.)
Figure C.1: Quantum circuit evaluating the average fidelity $F_n(\psi)$ between the perturbed and unperturbed maps $U$ and $U_p = UP$. The gates $R_k$ are $\pi/2$ rotation in the Bloch sphere around axis $k = x$ or $y$. When $k$ is set to $x$, we get the real part of $\text{Tr}\{(U^n)\dagger U^n_p\}/N$ while $k = y$ yields the imaginary part. The unitary operator $P$ is applied conditionally: when the probe qubit is in state $|1\rangle$, the unitary $P$ is applied to the lower register while no transformation is performed when the state of the probe qubit is $|0\rangle$.

This algorithm thus provides an exponential speed-up over all known classical procedures and uses a single bit of quantum information. Furthermore, it eliminates any cost of averaging the fidelity over a random set of initial states, as this averaging is done directly.

In order to implement certain unitary maps on $K$ qubits efficiently, it is necessary to introduce a number $K_a$ of ancillary qubits (a “quantum work-pad”) in the fiducial state $|\psi_0\rangle$. Ancillary qubits in pseudo-pure states can be used in the DQC1 setting. As a first step of the computation, part of the polarization of the probe qubit of Eq. C.5 can be transferred to ancillas initially in maximally mixed states. Thus, as long as the size $K_a$ of the work-pad is at most poly-logarithmic in $K$, the algorithm remains efficient.

**Entanglement**

Perhaps the most surprising feature of the quantum algorithm as it is presented in Fig. C.1 is that the probe never gets entangled with the system throughout the computation. To show this, consider a generalized version of the circuit of Fig. C.1 where the $P$’s and the $U$’s are free to differ at each iteration, i.e. at step $j$, we apply $P_j$ conditionally on the probe qubit, followed by $U_j$. This generalization is necessary since the controlled $P$ gate will in general be decomposed as a sequence of elementary controlled and regular gates [BBC+95a]. Initially, the probe qubit is in state $\alpha|0\rangle + \beta|1\rangle$. After $k$
steps, the state of the QIP is
\[
\rho_k = \frac{1}{N} \left\{ |\alpha|^2 |0\rangle \langle 0| \otimes \mathbb{I} + \alpha \beta^* |1\rangle \langle 1| \otimes S^\dagger + \alpha^* \beta |1\rangle \langle 0| \otimes S + |\beta|^2 |1\rangle \langle 1| \otimes \mathbb{I} \right\} \quad (C.9)
\]

where \( S = U_k P_k \ldots U_2 P_2 U_1 P_1 U_1^\dagger U_2^\dagger \ldots U_k^\dagger \). Decomposing this state in the eigenbasis of the unitary matrix \( S |\phi_j\rangle = e^{i s_j} |\phi_j\rangle \), we get
\[
\rho_k = \frac{1}{N} \sum_j |\alpha_j\rangle \langle \alpha_j| \otimes |\phi_j\rangle \langle \phi_j| \quad (C.10)
\]

where \( |\alpha_j\rangle = \alpha |0\rangle + \beta e^{i s_j} |1\rangle \); the state is separable. Its separability supports the point of view that the power of quantum computing derives not from the special features of quantum states – such as entanglement – but rather from fundamentally quantum operations [SC99a, LCNV01a].

Our algorithm also illustrates the relation between decoherence rate and the dynamical properties of the environment [BKZ03a]. Consider the probe qubit of Fig. C.1 as a quantum system interacting with a complex environment consisting of \( K \) two-level systems. After a “time” \( n \), the state of the system is given by tracing out the \( K \) environmental qubits from Eq. C.9. The diagonal elements of the reduced density matrix \( |\alpha|^2 \) and \( |\beta|^2 \) are left intact while the off-diagonal elements \( \alpha \beta^* \) and \( \alpha^* \beta \) are decreased by a factor \( |\text{Tr}\{S\}| \) which is roughly equal to \( \sqrt{F_n(\psi)} \). Thus, in the presence of a chaotic environment, the system will unavoidably decohere at a rate governed solely by the strength of the coupling. On the other hand, given a simple coupling to a regular environment, the system can maintain its coherence over a long period of time. This analogy also provides a very simple example of decoherence without entanglement [EP02a].

**Quantum probe**

On the circuit of Fig. C.1, only the perturbation gates \( P \) are conditioned on the state of the probe qubit. This suggests a dual interpretation of the algorithm as quantum circuit and quantum probe. On the one hand, \( U \) could be a known unitary transformation which is being simulated on the lower \( K \)-qubit register over which we have universal control. Then, the gate \( U \) would simply be decomposed as a sequence of elementary gates as prescribed in Refs. [Sch98b, GS01a, BCMS01a] for example. On the other hand, the lower register could be a real quantum system undergoing its natural evolution \( U \) which
might not even be known. Then, the probe qubit should really be regarded as a probe which is initialized in a quantum superposition, used to conditionally *kick* the system, and finally measured to extract information about the system under study. In this case, it is not necessary to have universal control over the lower register (the quantum system), we must simply be able to apply a conditional small unitary transformation to it.

**Numerical study**

Finally, Eq. C.8 provides a useful numerical tool that can be used to compute the *exact* average fidelity instead of estimating it by averaging over a finite random sample of initial states. In Ref. [EWL+02a], FD was illustrated on the quantum kicked top map $U_{QKT} = \exp\{-i\pi J_y/2\} \exp\{-ikJ_z^2/j\}$ acting on the $N = 2j + 1$ dimensional Hilbert space of angular momentum operator $\vec{J}$. The chosen perturbation operator was $P = \prod_{j=1}^{K} \exp\{-i\delta j^2/2\}$, a collective rotation of all $K$ qubits of the QIP by an angle $\delta$. The decay rate (governed by the Fermi golden rule in this regime) is $|V|^2 \delta^2 = 2.50 \delta^2$ for this perturbation [EWL+02a]. $F_n(\psi)$ was estimated in both chaotic ($k = 12$) and regular ($k = 1$) regimes of the kicked top by averaging over 50 initial states. We reproduce these results on Fig. C.2 and compare them with the exact average Eq. C.8 and theoretical prediction $e^{-|V|^2 \delta^2 n}$. The random sample is in good agreement with the exact average except that the former shows fluctuations. Furthermore, the decay in the chaotic regime is in excellent agreement with the Fermi golden rule, while it is considerably slower in the regular regime.

**Conclusion**

We have presented an efficient quantum algorithm which computes the average FD of a quantum map under perturbation using a single bit of quantum information. The quantum circuit for this algorithm establishes a link between decoherence by a chaotic environment and FD. Using a special case of our theorem, we have numerically evaluated the exact average FD for the quantum kicked top, and found good agreement with previous estimations using random samples. Although we have mainly motivated our algorithm for the study of quantum chaos, we believe that it has many other applications such as characterizing noisy quantum channels and computing correlation functions.
C.2. Exponential speed-up with a single bit of quantum information: Measuring the average fidelity decay

Figure C.2: Fidelity decay $F_n(\psi)$ averaged over 50 initial computational basis states for $U_{QKT}$ in a regular regime ($k = 1$, squares) and chaotic regime ($k = 12$, circles). The dashed lines represent the exact average Eq. C.8 and the full line shows the exponential decay at the Fermi golden rule rate $|V|^2/\delta^2$.

for many-body systems. We have also shown that our algorithm can be viewed as a special experiment where a quantum probe is initialized in a superposition and used to conditionally kick the system under study. This type of quantum information science byproduct might open the horizon to new types of experimental measurements where a small QIP is used to extract information from the quantum system under study. Finally, the effective speed-up despite the limited presence of entanglement – in particular its complete absence between the quantum probe and the mixed register – is a step forward in our understanding of the origin of quantum-computational speed-up.

We thank J. Emerson, G. Milburn, J.P. Paz, and W.H. Zurek for helpful discussions. We also acknowledge the Benasque Center for Science where this work was initiated. This work was supported in part by NSERC, ARDA, CIAR, ACI sécurité informatique, and by the Department of Energy, under contract W-7405-ENG-36.
C.3. Estimation of the Local Density of States on a Quantum Computer†

Joseph Emerson¹, Seth Lloyd², David Poulin³, and David Cory¹

¹Department of Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, MA, 02139, USA.
²Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA, 02139, USA.
³Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada.

Abstract: We report an efficient quantum algorithm for estimating the local density of states (LDOS) on a quantum computer. The LDOS describes the redistribution of energy levels of a quantum system under the influence of a perturbation. Sometimes known as the “strength function” from nuclear spectroscopy experiments, the shape of the LDOS is directly related to the survival probability of unperturbed eigenstates, and has recently been related to the fidelity decay (or “Loschmidt echo”) under imperfect motion-reversal. For quantum systems that can be simulated efficiently on a quantum computer, the LDOS estimation algorithm enables an exponential speed-up over direct classical computation.

A major motivation for the physical realization of quantum information processing is the idea, intimated by Feynman, that the dynamics of a wide class of complex quantum systems may be simulated efficiently by these techniques [Llo96a]. For a quantum system with Hilbert space size $N$, an efficient simulation is one that requires only Polylog$(N)$ gates. This situation should be contrasted with direct simulation on a classical processor, which requires resources growing at least as $N^2$. However, complete measurement of the final state on a quantum processor requires $O(N^2)$ repetitions of the quantum simulation. Similarly, estimation of the eigenvalue spectrum of a quantum system admitting a Polylog$(N)$ circuit decomposition requires a phase-estimation circuit that grows as $O(N)$ [AL97a]. As a result there still remains the important problem of devising methods for the efficient readout of those characteristic properties that are of practical interest in the study of complex quantum systems. In this Letter we introduce an efficient quantum algorithm for estimating, to $1/$Polylog$(N)$ accuracy, the local density of states (LDOS), a quantity of central interest in the description of both many-body and complex few-body systems. We also determine the class of physical problems for which the LDOS estimation algorithm provides an exponential speed-up over known classical algorithms given this finite accuracy.

The LDOS describes the profile of an eigenstate of an unperturbed quantum system over the eigenbasis of perturbed version of the same quantum system. In the context of many-body systems the LDOS was introduced to describe the effect of strong two-particle interactions on the single particle (or single hole) eigenstates [Wig55a, Wig57a, BM69a, FGG+94a, GS97a, FI00a]. More recently, the LDOS has been studied to characterize the effect of imperfections (due to residual interactions between the qubits) in the operation of quantum computers [GS00a, BCM+02a]. This profile plays a fundamental role also in the analysis of system stability for few-body systems subject to a sudden perturbation [CH00a, CBH01a, VC03a], such as the onset of an external field, and has been studied extensively in the context of quantum chaos and dynamical localization [BGI98a, Izr90a]. Quite generally the LDOS is related to the survival probability of the unperturbed eigenstate [CH00a, CBH01a, VC03a, BM69a, JSB01a], and there has been considerable recent effort to understand the conditions under which the LDOS width determines the rate of fidelity decay under imperfect motion-reversal (“Loschmidt echo”) [JSB01a, EWL+02a, CLM+01a, WC02a].

A number of theoretical methods have been devised to characterize the LDOS for
C.3. Estimation of the Local Density of States on a Quantum Computer

complex systems. These methods include banded random matrix models \cite{Wig55a, Wig57a, FM95a, JS95a, FCI+96a}, models of a single-level with constant couplings to a “picket-fence” spectrum \cite{BM69a, GAC+97a}, and perturbative techniques with partial summations over diagrams to infinite order \cite{CDG92a}. Under inequivalent assumptions these approaches affirm a generic Breit-Wigner shape for the LDOS profile,

\begin{equation}
\eta_{BW}(\phi) \propto \frac{\Gamma}{\phi^2 + \Gamma^2/4}.
\end{equation}

However, the extent to which these methods correctly describe any real system is generally not clear \cite{CH00a, CBH01a, VC03a, WVP+02a}, and therefore direct numerical analysis is usually necessary. It is worth stressing here that direct numerical computation of the LDOS requires the diagonalization of matrices of dimension $N$, and therefore demands resources that grow at least as $N^2$. Of course only coarse-grained information about the LDOS is of practical interest since one cannot even store the complete information efficiently for large enough systems. However, for generic systems there is no known numerical procedure that can circumvent the need to manipulate the $N \times N$ matrix in order to extract even coarse information about its LDOS. In this Letter we report a quantum algorithm which enables estimation of the LDOS to $1/\text{Polylog}(N)$ accuracy with only $\text{Polylog}(N)$ resources.

To specify the algorithm we represent the unperturbed quantum system by a unitary operator $U$, which may correspond either to a Floquet map, or to evolution under a time-independent Hamiltonian,

\begin{equation}
U = \exp(-iH_0 \tau)
\end{equation}

We represent the perturbed quantum system by the unitary operator $U(\sigma)$, which we express in the form,

\begin{equation}
U(\sigma) = \exp(-i\delta V)U,
\end{equation}

where $\delta$ is some dimensionless parameter and $V$ is a Hermitian perturbation operator. The variable $\sigma$ denotes an effective “perturbation strength” taking into account both the parameter $\delta$ and the size of the matrix elements of the perturbation,

\begin{equation}
\sigma^2 = \delta^2 |\langle \phi_j | V | \phi_{j'} \rangle|^2
\end{equation}

where the average is taken only over directly coupled eigenstates. Let $U|\phi_j\rangle = \exp(-i\phi_j)|\phi_j\rangle$, and $U(\sigma)|\phi_k(\sigma)\rangle = \exp(-i\phi_k(\sigma))|\phi_k(\sigma)\rangle$ denote the eigenphases and eigenstates of the
unperturbed and perturbed systems respectively. The LDOS for the \(j\)'th eigenstate of \(U\) is then,
\[
\eta_j(\phi) = \sum_k P(\phi_k(\sigma)|\phi_j) \delta(\phi - (\phi_k(\sigma) - \phi_j)),
\]
where the transition probabilities,
\[
P(\phi_k(\sigma)|\phi_j) = |\langle \phi_k(\sigma)|\phi_j \rangle|^2,
\]
are the basic quantities of interest.

The coarse-grained distribution,
\[
P(\Delta_l|\phi_j) = \sum_{\phi_k(\sigma) \in \Delta_l} P(\phi_k(\sigma)|\phi_j),
\]
is a just the sum over the probabilities for those perturbed eigenphases \(\phi_k(\sigma)\) lying within a band \(\Delta_l\). This band is centered about angle \(2\pi l/M\), with width \(\Delta = 2\pi/M\), and the integer \(l\) ranges from 0 to \(M - 1\). Similarly, an averaging over neighboring unperturbed eigenstates is often carried out to remove the effects of atypical states. The combination of both operations yields the probability distribution,
\[
P(\Delta_l|\Delta_m) = N_m^{-1} \sum_{\phi_k(\sigma) \in \Delta_l} \sum_{\phi_j \in \Delta_m} P(\phi_k(\sigma)|\phi_j),
\]
where the normalization constant \(N_m\) is just the number of unperturbed eigenphases in the angular range \(\Delta_m\). In practice one must choose \(M\) to be \(O(\log(N))\) since otherwise the measured LDOS \(\eta\) would contain an exponential amount of information and therefore could not be processed efficiently.

We now describe the algorithm for estimating the LDOS on a quantum processor. The circuit for this algorithm is depicted in Fig. C.3. The lower register implements the perturbed and unperturbed maps \(U\) and \(U(\sigma)\), requiring \(n_q = O(\log_2(N))\) qubits. The upper register holds the \(m_q = \log_2(M)\) ancillary qubits which fix the precision of the phase-estimation algorithm. The upper register always starts out in the ‘ready’ state \(|0\rangle\). The appropriate choice of initial state \(\rho\) in the \(n_q\) register will depend on the context, as explained below. For the moment we assume the lower register is prepared in a pure state, \(\rho = |\psi_o\rangle\langle\psi_o|\). The first step of the algorithm involves estimating the eigenphases of the unperturbed operator \(U\). This takes the initial state through the
Figure C.3: Circuit diagram for measuring the local density of states, consisting of two successive phase-estimation circuits on different operators. The diagonal line denotes a bundle of qubits and the thick vertical bar denotes a projective measurement of the quantum state in the computational basis. The upper register contains \( m_q = \log(M) \) qubits and the operations on the lower register are applied conditionally \( m \) times, where the integer \( m \in [0, M-1] \) is determined from the binary representation of the computational basis states in the upper register.

sequence, 

\[
|0\rangle \otimes |\psi_o\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} |m\rangle|\psi_o\rangle \\
\rightarrow \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} |m\rangle(U)^m|\psi_o\rangle \\
= \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} |m\rangle \sum_{j=0}^{N-1} c_j \exp(i\phi_j m)|\phi_j\rangle \\
\rightarrow \sum_{j=0}^{N-1} c_j |m_j\rangle|\phi_j\rangle, \quad \text{(C.19)}
\]

where \( c_j = \langle \phi_j |\psi_o\rangle \). The state \( m_j \) is the nearest \( m_q \)-bit binary approximation to the \( j \)'th eigenphase of \( U \)

\[
\tilde{\phi}_j = 2\pi m_j/M \simeq \phi_j. \quad \text{(C.20)}
\]

Upon strong measurement of the \( m_q \) register one obtains and records a single outcome \( m \), and the state of \( n_q \) register must then be described by (viz, ‘collapsed to’) the updated pure state,

\[
|\psi(\Delta_m)\rangle = \sum_{\phi_j \in \Delta_m} \tilde{c}_j |\phi_j\rangle, \quad \text{(C.21)}
\]

corresponding to the subspace of eigenstates with eigenphases in the band \( \Delta_m \) of width \( \Delta = 2\pi/M \) about the phase \( 2\pi m/M \). To keep normalization the coefficients have been
rescaled as follows,
\[ \tilde{c}_j = \frac{c_j}{\left( \sum_{\phi_j \in \Delta_m} |c_j|^2 \right)^{1/2}} \]  
(C.22)

Next we reset the \( m_q \) qubit register to the ready state and run the phase-estimation algorithm on the operator \( U(\sigma) \), producing the final state,
\[ |\psi\rangle = \sum_{\phi_j \in \Delta_m} \tilde{c}_j \sum_{k=0}^{N-1} b(k|j) |m_k\rangle \otimes |\phi_k(\sigma)\rangle, \]
(C.23)

where \( \tilde{\phi}_k(l) = 2\pi m_k/M \) is an \( m_q \)-bit approximation to \( \phi_k(\sigma) \). The complex coefficients \( b(k|j) = \langle \phi_j|\phi_k(\sigma)\rangle \) are the inner product of the perturbed and unperturbed eigenstates. Measurement of the \( m_q \) register now reveals an outcome \( l \), associated with the eigenphases in the angular range \( 2\pi l/M \pm \Delta/2 \). The outcome \( l \) occurs with probability,
\[ P_{\psi_o}(l|m) = \sum_{\phi_k \in \Delta_l} \left| \sum_{\phi_j \in \Delta_m} \tilde{c}_j b(k|j) \right|^2 \]
(C.24)

which is conditional on the earlier outcome \( m \) and the choice of initial state.

We now specify how the initial state may be chosen to eliminate unwanted fluctuations arising from the variables \( \tilde{c}_j \) in Eq. C.24. Before describing the general solution we consider first a special case of particular interest: when a known eigenstate of \( U \) may be prepared efficiently. Such an initial state may be prepared (or well approximated) by an efficient circuit when \( U \) consists of some sufficiently simple integrable system (e.g., a non-interacting many-body system). In this case we have \( \tilde{c}_j = \delta_{jk} \), and the final probability distribution Eq. C.24 reduces exactly to the (coarse-grained) kernel Eq. C.17,
\[ P_{\phi_k}(l|m) \rightarrow P(\Delta_l|\phi_k). \]
(C.25)

When the eigenphase associated to the prepared eigenstate is known to sufficient accuracy (so that \( m \) is known), it is not even necessary to perform the first phase estimation routine. In the general case of a generic quantum system, it is sufficient to prepare the maximally mixed state as the initial state, in which case the final probability distribution reduces exactly to the (coarse-grained and averaged) probability kernel Eq. C.18, i.e.,
\[ P_{1/N}(l|m) = \frac{1}{N_m} \sum_{\phi_k(\sigma) \in \Delta_l} \sum_{\phi_j \in \Delta_m} P(\phi_k(\sigma)|\phi_j). \]
(C.26)
This probability kernel contains all the information needed to compute the (coarse-grained and averaged) LDOS, \( \eta_m(2\pi k/M) = \sum_l P(l|m)\delta_{k,(l-m)} \), completing our derivation.

The algorithm described above remains efficient provided that the quantum maps \( U \) and \( U_\delta \) admit Polylog(\( N \)) gate decompositions. Such decompositions have been identified both for many-body systems with local interactions and for a wide class of few-body quantized classical models. As mentioned earlier, for practical purpose \( M \) should be Polylog(\( N \)) so the overall circuit of Fig. C.3 is indeed efficient for such systems.

We now turn to the question of how many times \( K \) the algorithm must be repeated to arrive at interesting physical conclusions about the final probability distribution. This issue arises because the final probability distribution is not measured directly on the quantum processor; rather, it governs the relative frequency of outcomes obtained in each repetition of the algorithm. Indeed, it is by repeating the algorithm illustrated in Fig. C.3 and accumulating joint statistics of the \( l \) and \( m \) outputs that one can estimate the parent distribution \( P(l|m) \). The accuracy of this estimation depends on the number of times \( K \) the distribution is sampled. In order to bound \( K \) it is convenient to cast the physical problems related to the LDOS in terms of hypothesis testing. We consider the important case of testing which of two candidates distributions \( \eta_1 \) or \( \eta_2 \) best describes the LDOS of a given system and a given perturbation. For example, one might be testing whether the Lorentzian has one of two candidate widths, or whether the profile is Gaussian or Lorentzian. Only when \( K \leq \text{Polylog}(N) \) will the overall computation remain efficient. This problem is resolved in general by the Chernoff bound [CT91a].

A random variable is distributed according to either \( P_1(x) \) or \( P_2(x) \), and we wish to determine which distribution is the right one. Then, the probability \( P_e \) that we make an incorrect inference decreases exponentially with the number of times \( K \) the variable was sampled: \( P_e \leq \lambda^K \). Here, \( 0 \leq \lambda \leq 1 \) is a measure of similarity between distributions defined as

\[
\lambda = \min_{0 \leq \alpha \leq 1} \sum_x P_1(x)^\alpha P_2(x)^{(1-\alpha)}; \tag{C.27}
\]

in particular, \( \lambda \) is bounded above by the fidelity between \( P_1 \) and \( P_2 \). Thus, a constant error probability \( \epsilon \) requires a sample of size \( K = \log(\epsilon)/\log(\lambda) \). Therefore, as long as the concerned distributions are at a Polylog(\( N \)) distance, i.e. \( 1 - \lambda \geq 1/\text{Polylog}(N) \), they can be distinguished efficiently. We note that the test can be inconclusive when
both hypothesis are equally likely to describe the underlying physics.

Efficient application of the LDOS algorithm under these restrictions may be illustrated explicitly by working through a problem of practical interest from the recent literature. We consider the problem of testing whether the Breit-Wigner profile Eq. C.11 applies when a given quantized classically chaotic model is subjected to a perturbation of interest. From the BGS conjecture [BT77a, BGS84a] and studies of (banded) random matrix models [Wig55a, Wig57a, FM95a, JS95a, FCI+96a], it is generally expected that for fully chaotic models with generic perturbations Eq. C.11 applies with,

$$\Gamma(\sigma) = 2\pi\sigma^2\rho_E,$$

provided that the effective perturbation strength lies in the range,

$$1 \ll \sigma\rho_E \ll \sqrt{b},$$

where $b$ is the bandwidth of the perturbation in the ordered eigenbasis of $U$ and $\rho_E$ is the level density. It should be stressed that $\Gamma$ may be estimated a priori if the perturbation is known [EWL+02a, FM95a, JS95a]. Deviations from this hypothesis can arise for a wide variety of reasons (i.e., integrable or mixed classical dynamics in the unperturbed or perturbed system, non-generic properties of the perturbation, hidden symmetries, etc) and therefore analysis of the LDOS remains an active area of numerical study for both dynamical models [BGI98a, WVP+02a] and real systems [FGG+94a].

The lower bound of Eq. C.29 is determined from the breakdown of perturbation theory and leads to a width $\Gamma$ that decreases linearly with $N$. Since the circuit can only efficiently resolve the LDOS with accuracy $1/{\text{Polylog}}(N)$, the BW profile with width $\Gamma = O(N^{-1})$ may not be verified efficiently near this lower bound. However, near the upper bound of Eq. C.29 the validity of the BW profile may be tested efficiently. In the case of fully chaotic models one has $b = N/2$ and the upper bound for $\Gamma$ is therefore $O(1)$. Hence the validity of Eq. C.11 provides a hypothesis which may be tested efficiently for any perturbation such that $1/{\text{Polylog}}(N) \ll \Gamma(\sigma) \ll O(1)$. Near this bound one can also determine whether the chaotic model exhibits dynamical localization, since in this case one has a bandwidth $b \ll N/2$ and the LDOS will cease to maintain the BW profile when $b\rho_E^{-1} \ll \Gamma(\sigma) \ll O(1)$. Indeed for some models the localization length $l$ of the eigenstates scales as $l \simeq O(1)$ [CM03a], and hence this length may be estimated using the LDOS algorithm with only Polylog($N$) resources.
In summary we have reported an algorithm for efficiently estimating the LDOS of a quantum system subject to perturbation. There is wide range of contexts in which important coarse features of the LDOS, such as the width, may be estimated with only Polylog($N$) resources. We have described in detail the important problem of testing the Breit-Wigner hypothesis as one example for which the LDOS estimation algorithm gives an effective exponential speed up over classical computation.

We are grateful to D. Shepelyansky and Y. Weinstein for helpful discussions. This work was supported by the NSF and CMI.
C.4. Testing integrability with a single bit of quantum information†

David Poulin\textsuperscript{1,2}, Raymond Laflamme\textsuperscript{1,2}, Gerard J. Milburn\textsuperscript{3}, and Juan Pablo Paz\textsuperscript{4,5}
\textsuperscript{1} Perimeter Institute for Theoretical Physics, 35 King Street N., Waterloo, ON, N2J 2W9, Canada.
\textsuperscript{2} Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada.
\textsuperscript{3} Centre for Quantum Computer Technology, School of Physical Science, The University of Queensland, QLD 4072 Australia.
\textsuperscript{4} Departamento de Física “J.J. Giambiagi”, FCEN, UBA, Pabell on 1, Ciudad Universitaria, 1428 Buenos Aires, Argentina.
\textsuperscript{5} Theory Division, MS B213, Los Alamos National Laboratory, Los Alamos, NM 87545 USA.

Abstract: We show that deterministic quantum computing with a single bit (DQC1) can determine whether the classical limit of a quantum system is chaotic or integrable using $O(N)$ physical resources, where $N$ is the dimension of the Hilbert space of the system under study. This is a square root improvement over all known classical procedures. Our study relies strictly on the random matrix conjecture. We also present numerical results for the nonlinear kicked top.

Overview

After an initial triumph at solving mathematical problems (see [NC00a] for an overview), a large fraction of the researches in the field of quantum information processing has shifted to its original motivation: the simulation of quantum systems [Fey82a]. It is now well established [Llo96a, OGK+01a, SOG+02a] that the evolution produced by certain classes of Hamiltonians can be simulated efficiently on a universal quantum processor. However, extracting useful information from the physical simulation is a problem whose complexity has been underestimated. Indeed, the ability to simulate the dynamics of a system does not grant one with the ability to evaluate efficiently all physical quantities of interest. These quantities (e.g. spectral properties) are usually measured experimentally on a (exponentially) large number of physical systems — macroscopic samples. A direct quantum simulation, on the other hand, can only reproduce the statistical output of a single quantum system which yields drastically less information than what is learned from costly classical simulations. Thus, it is not clear at this point whether quantum simulators can always outperform their classical analogues.

Some of these spectral properties play a central role in the study of quantized chaotic systems. One particular question of interest is whether the classical limit of a quantum system exhibits regular or chaotic motion. It has became widely accepted (see [Haa01a, Sto99a] and references therein) that the answer to this question is hidden in some spectral properties of the system, which can be reproduced by those of canonical random matrices with the appropriate symmetries. Given a description of the Hamiltonian of the system, the best known algorithms evaluating these “signatures of chaos” require classical computing resources which grow at least as fast as \( N^2 \), the square of the dimension of the Hilbert space of the system under study. Indeed, a close inspection of these algorithms show that they require either matrix multiplication, diagonalization, or evaluation of a determinant [Haa01a]. Since such a growth is intractable on any conventional computer (remember that \( N \) grows exponentially with the size of the physical system), it is quite natural to try to tackle this problem with a quantum computer. In recent years, this interest has lead to the demonstration that the standard model of quantum computation can simulate efficiently the dynamics of a few quantized chaotic models [Sch98b, GS01a, BCMS01a]; unfortunately, none of these proposals indicate how to circumvent the measurement problem mentioned above.

Recent work by Emerson et al. [EWL+02a] proposes to study statistical properties
of the system's eigenvectors relative to a perturbation as a signature of chaos. They also provide an efficient procedure to measure these statistics using the standard model of quantum computation. Their motivation for this work was to test the validity of the signature. Indeed, it is not clearly established that this signature is universal, perturbation independent and, most importantly that the decay time does not scale with the size of the system.

Here, we concentrate on a different model (presumably weaker): deterministic quantum computation with a single pseudo pure bit (DQC1) which was introduced in [KL98b]. In this setting, the initial state of the $K+1$ qubits computer is $\rho = \left\{ \frac{1-\epsilon}{2} \mathbb{I} + \epsilon |0\rangle \langle 0| \right\} \otimes \frac{1}{2^K} \mathbb{I}$ where $0 < \epsilon \leq 1$ is a constant. Note that, from a computational complexity point of view, this is equivalent to a model where the state of the first qubit is pure while the other ones are completely random; we shall therefore assume that $\epsilon = 1$ in the remaining of the paper. The final answer is given by a finite accuracy evaluation of the average value of $\sigma_z$ on the first qubit. As for the dynamics, we assume that we are gifted with the ability to exert coherent control over one and two qubits at a time. This model is of particular interest since it is weaker than the computational model offered by liquid state nuclear magnetic resonance (NMR) quantum computing [CLK+00a]. Such a computing device, we shall show, can test for integrability using $O(N)$ physical resources, given that the dynamics of the system of interest is efficiently simulatable on the standard model of quantum computation without ancillary pure qubits (or, more precisely, with no more than $O(\log K)$ ancillary pure qubits).

In order to do so, we must first relate the theory underlying the spectral property at the heart of our study; this is done in Sec. C.4.2. We then show how it can be evaluated with $O(N)$ physical resources in the DQC1 model. In Sec. C.4.4, we present numerical results for canonical random matrices as well as for a physical map, the nonlinear kicked top. Finally, we conclude with a summary of our results and discussion of possible extensions.

**Level distribution**

In the theory of quantum chaos, a key role is played by the statistics of eigenvalues [Haa01a, Sto99a]. In the case of systems with a periodically time varying Hamiltonian the central dynamical object is the Floquet operator, $\hat{F} = \hat{T}[\exp\{-i \int_0^T H(t)dt\}]$, that maps the state from one time to a time exactly one modulation period $T$ later, $\hat{T}$ is
the time ordering operator. The eigenvalues of $\hat{F}$ lie on the unit circle and may be parameterized in terms of eignephases, or quasi-energies, as $\hat{F}|\phi_j\rangle = e^{-i\phi_j}|\phi_j\rangle$.

The random matrix conjecture asserts that the statistics of eigenvalues of chaotic systems (dynamical systems and maps) is typically well modeled by the statistics of the eigenvalues of random matrices (hermitian Hamiltonians and unitary Floquet operators) with the appropriate symmetries [Haa01a, Sto99a]. While many important mathematical results underpin the conjecture, a rigorous proof is lacking and support rests on a very large accumulation of numerical results.

An integrable system, by definition, possesses as many symmetries — constant of motion — as degrees of freedom. One can thus write the system’s Hamiltonian as the direct sum of independent Hamiltonians acting on smaller subspaces; one for each values of the constants of motion. Some spectral properties of these Hamiltonians can thus be reproduced by those of matrices that are the direct sum of independent random Hermitian operators. The distribution characterizing the entire spectrum is therefore given by the superposition of many independent spectra; as a consequence, the correlations between levels vanish. Thus, one might expect that the nearest neighbors level spacing distribution (LSD) follow a Poisson law $\text{prob}(\phi_{j+1} - \phi_j = S) = P(S) \sim e^{-\Gamma S}$, a straightforward consequence of their statistical independence. This is indeed observed experimentally, numerically, and most importantly can be derived formally [BT77a].

On the other hand, chaotic systems possess no or just a few symmetries. It can be shown [Haa01a] that the LSD — aside from the systematic degeneracy following the symmetries — obeys a power law $P(S) \sim S^\beta e^{-\alpha S^2}$. The parameter $\beta$ characterizes the symmetries of the system; it is equal to 1 when the system possesses a time reversal symmetry and some geometric invariance, 2 when it has no symmetries, and 4 when it has a time reversal symmetry with Kramer’s degeneracy. Similarly, we will refer to the Poisson ensemble — the characteristic ensemble of integrable systems — as $\beta = 0$.

The exact form of the LSD is not relevant to us; we shall capitalize on the crucial distinct behavior of $P(S \to 0)$ for chaotic and regular systems. In the former case, $P(S)$ reaches a minimum at $S = 0$: the levels tend to repel each other. In the latter case, $P(S)$ is maximal at $S = 0$, a consequence of the levels statistical independence called clustering.

With these considerations, one can predict the behavior of the ensemble average
form factors

\[ T_n = \left| \text{Tr}\{\hat{F}^n\} \right|^2 = \left| \sum_{j=1}^{N} e^{-i\phi_j} \right|^2 \]  

(C.30)

from which most spectral properties can be extracted. For regular systems, \( \text{Tr}\{\hat{F}\} = \sum_j e^{-i\phi_j} \) behaves like the end point of a random walk in the complex plane: each step having unit length and uncorrelated random orientation \( \phi_j \). After \( N \) steps, the average distance from the origin is expected to be \( \sqrt{N} \) so we should find \( \bar{T}_1 = N \). For times \( n > 1 \), the analysis is identical; if the angles \( \{\phi_j\} \) are statistically independent, then so are \( \{\phi_j^{(n)} = n\phi_j \text{mod}(2\pi)\} \), \( n \) taking positive integer values. We conclude that the ensemble average form factors of integrable systems should be time independent and equal to \( N \).

For chaotic systems, more elaborate calculations are required for the ensemble average form factors. They can be found in [Haa01a]; here we shall simply give an approximate result for \( 0 < n < N \) (accuracy of order \( 10^{-2} \)) known as the Wigner surmises:

\[
\bar{T}_n = \begin{cases} 
2n - n \sum_{m=1}^{n} \frac{1}{m+(N+1)/2} & \text{for } \beta = 1 \\
 n & \text{for } \beta = 2 \\
n \frac{N-1}{2} \sum_{m=1}^{n} \frac{1}{N^{1/2}-m} & \text{for } \beta = 4 
\end{cases} 
\]  

(C.31)

Although simple arguments could not have indicated the exact behavior of these form factors, we could have guessed their general form: they are initially very small \( \bar{T}_1 \ll N \), and, as \( n \) grows, they reach the same value as the Poisson ensemble. Here, \( \text{Tr}\{\hat{F}\} \) is analog to a anti-correlated random walk in the complex plane composed of \( N \) unit steps. As a consequence of level repulsion, each steps tend to be oriented in different directions; the probability of finding two steps oriented within an angle \( \epsilon \) decreases as \( \epsilon^{\beta+1} \). Thus, the distance from the origin after \( N \) of these anti-correlated steps should definitely be smaller than \( \sqrt{N} \) which is the expected value for uncorrelated steps. As \( n \) grows, the phases \( n\phi_j \text{mod}(2\pi) \) get wrapped around the unit circle; the effect is analogue to superposing \( n \) independent spectral distributions, blurring out the correlations. When \( n \sim N \), one should thus expect a behavior similar to the Poisson ensemble.

It should be noted that the few symmetries of a chaotic system may slightly affect the predictions of Eq. C.31. The average \( \bar{T}_n \) were evaluated for fixed values of the constant of motion. In what follows, we shall often neglect this point for sake of simplicity. Nevertheless as long as the number of invariant subspaces is small (\( \ll \sqrt{N} \)) this omission
will not affect our conclusions. For example, if a chaotic system possesses a symmetry which breaks its Hilbert space into $k$ equal invariant subspaces, the small $n$ behavior $T_n \simeq n$ will be transformed into $T_n \simeq k^2 n \ll N$, which is all that really matters to us. One can circumvent this issue when some exact symmetries of the system are known: it suffices to simulate the dynamics of the system within an invariant subspace.

In the light of this analysis, it may seem that form factors constitute a powerful tool to distinguish between classically regular and chaotic systems. In particular, $T_n$ should clearly identify each regime for small values of $n$. Nevertheless, the form factor $T_n$ of a fixed Floquet operator $\hat{F}$ will generally fluctuate about the ensemble average $\overline{T_n}$. Thus, we seek a signature of an ensemble property on a single element drawn from this ensemble.

The solution is to use a version of the ergodic theorem. If we normalize out the explicit time dependence of the form factors, an average over a time interval $\Delta n$ reproduces the effect of an ensemble average. More precisely, one can show [Haa01a] that

$$\langle T_n/T_n \rangle = \frac{1}{\Delta n} \sum_{n'=n-\Delta n/2}^{n+\Delta n/2} T_{n'}/\overline{T_{n'}}$$

(C.32)

converges to 1 with a variance $\sigma^2$ bounded by $1/\Delta n$. For large $N$, we can thus use the first $\Delta n \ll N$ form factors to determine whether the Floquet operator belongs to a polynomial or Poisson ensemble. Since the value of $\overline{T_n}$ — hence the matrix ensemble — are needed to compute Eq. C.32, we shall proceed by hypothesis testing: for which choice of $\overline{T_n}$ ($\overline{T_n} = N$ regular, $\overline{T_n} \simeq n$ chaotic) does Eq. C.32 converge to 1? In other words, we need to determine which of the two variables

$$t_0 = \frac{1}{\Delta n} \sum_{n=1}^{\Delta n} \frac{T_n}{N} \quad \text{or} \quad t_1 = \frac{1}{\Delta n} \sum_{n=1}^{\Delta n} \frac{T_n}{n}$$

(C.33)

is most probably drawn from a distribution centered at 1 with $1/\sqrt{\Delta n}$ standard deviation. If we restrict our attention to a regime where $\Delta n \ll N$, both hypothesis cannot have high probabilities simultaneously \(^5\). On the other hand, when the probabilities of both hypothesis are low, the test is inconclusive. Nevertheless, remember that the

---

\(^5\)It is important to note that $\Delta n$ needs not to increase with $N$, in fact it is quite the opposite. The probability of error scales like the overlap of two Gaussian distributions of width $\sigma = 1/\Delta n$ and centered about points $\mu_1$ and $\mu_2 \simeq N \mu_1$: clearly, this overlap decreases with $N$. 

---
presence of symmetries in a chaotic system shifts the value of the distribution by a factor $k^2$ where $k$ is the number of invariant subspaces. For $k^2 \ll N$, this should be clearly distinguishable from the value of a regular system. This should not be seen as a bug but a feature of our approach allowing one to estimate $k$, the number of invariant subspaces.

Applying this test to a particular dynamical system would require one to compute the spectrum of the Floquet operator. If one were to try and simulate a dynamical map on a quantum computer with $K$ qubits, a direct computation would require determining all $N = 2^K$ eigenvalues. In the next section we will construct a quantum circuit that would enable the form factors themselves to be extracted with $O(N)$ physical resources thus allowing a direct test of non-integrability that circumvented the need to explicitly compute all eigenvalues.

Quantum algorithm

The DQC1 algorithm evaluating the form factor is based on the idea reported in [MPS+02a] of using a quantum computer as a spectrometer. The circuit is shown at Fig. C.4 where $K = \lceil \log_2 N \rceil$. By hypothesis, we are able to efficiently simulate the dynamics of the system under study so the gate $\hat{F}^n$ only requires a polynomial (in $n$ and $K$) number of elementary gates to be constructed. Here, it is not $\hat{F}^n$ we wish to implement but a coherently controlled version of it, i.e. a linear gate acting on $K + 1$ qubits which applies $\hat{F}^n$ to the last $K$ qubits when the first qubit is in state $|1\rangle$ and doesn’t do anything when it is in state $|0\rangle$. Given the circuit for $\hat{F}^n$, standard techniques can be used to construct a controlled version of it at polynomial cost [BBC+95a].

It should also be emphasized that the $K$ qubits on which the Floquet operator
is applied generate a Hilbert space of dimension $2^K$ which might be larger than the simulated system’s Hilbert space. Thus, when applying $\hat{F}$ to those qubits, one really applies $\hat{F} \oplus U$ where ideally $U$ is the identity operator on $2^K - N$ states; it can be any other unitary operator as long as its trace can be evaluated. The effect of these extra dimensions will be to add a contribution $\text{Tr}\{U\}/N$ to the output signal which should be systematically subtracted as we shall henceforth assume.

The output of this computation will be the real and imaginary part of $(\text{Tr}\{\hat{F}^n\})/2^K$ when the last rotation is made about axis $k = x$ and $k = y$ respectively. Thus, our task is to distinguish between a signal whose amplitude is of order $1/N$ (chaotic dynamics) and one of order $1/\sqrt{N}$ (regular dynamics) which can be achieved using $O(N)$ physical resources. In the special case of NMR quantum computing, one can for example increase the size of the sample by a factor $N$ as the size of the system increases, or simply repeat the procedure $N$ times and sum up the outputs. We thus get a quadratic advantage over all known classical algorithms.

**Numerical results**

**Random Matrices**

Before applying our general proposal to a physical model, we give a numerical example illustrating the main results used from random matrix theory: the ergodic theorem of Eq. C.33. In order to estimate the average and variance of $t_0$ and $t_1$ in a given universal matrix ensemble, we draw many random matrices $U^{(k)}$ from the ensemble and numerically evaluate each quantity. As an example, we have generated 50 random matrices from the $\beta = 2$ ensemble — the set of unitary matrices with no symmetries. This is illustrated on Fig. C.5, where the matrices are of size $600 \times 600$. For each random matrix $U^{(k)}$ drawn from this ensemble, we can compute $t_1(U^{(k)})$ as functions of $\Delta n$. Two such curves (dashed) are plotted on Fig. C.5. By applying this procedure to many samples (here 50), we can estimate the average of $t_1$ and its fluctuations:

$$\langle t_1 \rangle = \frac{1}{50} \sum_{k=1}^{50} t_1(U^{(k)}), \quad \langle (t_1)^2 \rangle = \frac{1}{50} \sum_{k=1}^{50} [t_1(U^{(k)})]^2.$$ (C.34)

The average $\langle t_1 \rangle$ and mean deviation $\sigma = \sqrt{\langle (t_1)^2 \rangle - \langle t_1 \rangle^2}$ are also plotted on Fig. C.5 (heavy and light full line respectively): as expected, $t_1$ converges to 1 as $1/\sqrt{\Delta n}$. The same procedure can be applied to $t_0$; nevertheless, since $t_1$ does converge to 1 in this...
ensemble, $t_0$ obviously does not since it differs by a factor of roughly $N/\Delta n \simeq 20$ for the range of $\Delta n$ we have studied. Of course, this difference would vanish when $\Delta n$ approaches $N$ since the form factor of any universal ensemble converge to those of the Poisson ensemble (see Sec. C.4.2); this is why we must restrict our study to $\Delta n \ll N$. The same conclusions can be reached for the other ensembles characterizing chaotic systems, i.e. $\beta = 1, 2, \text{and} 4$.

![Figure C.5](image)

Figure C.5: The two dash lines show $t_1$ as a function of $\Delta n$ (Eq. C.33) for two random unitary matrices drawn from the ensemble $\beta = 2$. The heavy full line is the value of $t_1$ averaged over 50 such random matrices while the light line shows its variance, which drops as $1/\sqrt{\Delta n}$ as expected.

Similarly, had the matrices $U^{(k)}$ been drawn from the $\beta = 0$ ensemble — the set of matrices characterizing regular systems — we would have observed $t_0$ converging to 1 as $1/\sqrt{\Delta n}$ while $t_1$, smaller by a factor of roughly $\Delta n/N$, would roughly vanished. From these considerations, the hypothesis test “$t_0$ converges to 1” versus “$t_1$ converges to 1” allows us to discriminate between random matrices drawn from $\beta = 0$ and those drawn from one of the $\beta = 1, 2, \text{or} 3$, with a probability of error decreasing as $1/\sqrt{\Delta n}$. Thus, as long as the random matrix conjecture holds, it should also allow to discriminate between regular and chaotic motion.

*Kicked Top*

We now focus our attention on a physical model of great interest for its good agreement with random matrix theory: the nonlinear kicked top. We write the Floquet operator
in its most general form following Haake [Haa01a], \( \hat{F} = U_z U_y U_x \) with
\[
U_k = \exp \left\{ -i \frac{\tau_k J_k^2}{2j + 1} - i \alpha_k J_k \right\}
\] (C.35)

where the \( J_k, k = x, y, \) and \( z, \) are the canonical angular momentum operators. We conveniently define a parameter vector \( p = (\alpha_x, \alpha_y, \alpha_z, \tau_x, \tau_y, \tau_z) \). Some authors use a restricted form of this Floquet operator where only \( \tau_z \) and \( \alpha_y \) are non-zero. Since \([\hat{F}, J^2] = 0\), the value of the angular momentum \( j \) — which appears in Eq. C.35 — is conserved. The dimension of the Hilbert space is simply given by \( N = 2j + 1 \).

By adequately choosing the parameters \( p \), the kicked top can be either in a regular or chaotic regime, see [Haa01a] for more details. Thus, we can evaluate \( t_0 \) and \( t_1 \) of Eq. C.33 in both regimes and verify that they indeed allow to discriminate between them. This is presented on Figs. C.6 and C.7 for different values of the total angular momentum \( j \). On Fig. C.6, the system is in a regular regime; we have only plotted \( t_0 \) since \( t_1 \) is larger by a factor proportional to \( j \) so clearly does not converge to 1. Similarly, only the value of \( t_1 \) is exhibited of Fig. C.7. Notice that while the ergodic averaging decreases the fluctuations, it is not essential to discriminate between regular and chaotic. Indeed, the scale of the fluctuation is extremely small compared to \( j \) which is the factor by which \( t_0 \) and \( t_1 \) differ.

The analogy with a random walk in the plane can also be illustrated graphically. On Fig. C.8 we have plotted the sum of the eigenvalues vectorially. The apparent structure of the vectors is purely artificial, the eigenphases were ordered in increasing order (the sum of vectors is obviously a commutative operation); we have chosen this ordering to facilitate the presentation.

The effect of LSD are striking on Fig. C.8. The light vectors (chaotic regime) are arranged in an almost perfect circle; eigenphases tend to be equally separated. On the other hand, the heavy vectors (regular regime) are quite often aligned in an almost straight line; a manifestation of level clustering. As a consequence, the heavy vectors end up further apart from the origin than do the light vectors; on average, these distances differ by a factor \( \sqrt{N} \).

Finally, we can use the form factor to study the transition between regular and chaotic motion. To do so, we let the parameter vector continuously vary from its regular value to its chaotic value: \( p = (1 - \epsilon)p_r + \epsilon p_c \) (see figure captions C.6 and C.7). For \( \epsilon = 0 \), the expected value of \( t_0 \) is 1. As \( \epsilon \) increases, the system enters a chaotic regime;
C.4. Testing integrability with a single bit of quantum information

Figure C.6: Value of $t_0$ (Eq. C.33) of the kicked top in a regular regime $p_r = (0, 0, 1, 0, 0, 10)$ as in [Haa01a] for different values of $j$. Dashed curve: $\Delta n = 1$ so it is simply $\text{Tr}\{\hat{F}\}/N$. Full curve: To decrease the fluctuation, we have used the ergodic averaging over the first $\Delta n = 30$ normalized form factors $\text{Tr}\{\hat{F}_n\}/N, n = 1, 2, \ldots 30$.

Figure C.7: Value of $t_1$ (Eq. C.33) of the kicked top in a chaotic regime $p_c = (1.1, 1, 1, 4, 0, 10)$ as in [Haa01a] for different values of $j$. Dashed curve: $\Delta n = 1$ so it is simply $\text{Tr}\{\hat{F}\}$. Full curve: To decrease the fluctuation, we have used the ergodic averaging over the first $\Delta n = 30$ normalized form factors $\text{Tr}\{\hat{F}_n\}/n, n = 1, 2, \ldots 30$.

When chaos has fully developed, $t_0$ should vanish as $1/N$. This is indeed observed on Fig. C.9, where we have plotted $t_0$ as a function of $\epsilon$ for different system sizes. Moreover,
Figure C.8: Vectorial representation of eigenphases: $\sum_j (\cos \phi_j, \sin \phi_j)$ where the $\phi_j$ have been ordered in increasing order. The $\alpha$ and $\tau$ parameters of the Floquet operator Eq. C.35 are tuned so the system is in a regular regime (heavy vectors) and a chaotic regime (light vectors) as in Figs. C.6 and C.7. The value of $j$ is 20 so each curve contains 41 vectors.

The results indicate that the transition to chaos becomes more sensible as the size of the system increases.

Figure C.9: Value of $t_0$ (Eq. C.33) with $\Delta n = 30$ for different system size: Full heavy line $j = 50$; Dashed line $j = 100$; Light full line $j = 200$. 
Conclusion

We have shown that, using a single bit of quantum information, we can test whether the spectrum of a unitary matrix obeys a Poisson or polynomial law. Under the random matrix conjecture, this can be used to determine whether the system has a regular or chaotic behavior in its classical limit. The idea relies on estimating the averaged form factor using the ergodic theorem which roughly states that a time average can reproduce an ensemble average. The form factors in a regular and chaotic regime differ by a factor of $\sqrt{N}$ and the output signal of our computation decreases as $1/N$: the required physical resources thus scale as $N$. This is a quadratic improvement over all known classical algorithms. We are currently investigating a different signature of quantum chaos which might not suffer from this signal loss and hence, could offer an exponential speed up.

This result gives a new insight on the nature of the potential computational speed up offered by quantum mechanics. In particular, it provides a strong argument towards the computational power of mixed states quantum computing.

We acknowledge Harold Ollivier for stimulating discussions and careful reading of this manuscript, and Howard Wiseman for pointing out an error in an earlier version of this work. DP is financially supported by Canada’s NSERC, and RL by NSERC and CIAR.
C.5. Compatibility of quantum states†

David Poulin and Robin Blume-Kohout
Los Alamos National Laboratory, Theoretical Division,
MS-B210, Los Alamos, New Mexico 87545, USA.

Abstract: We introduce a measure of the compatibility between quantum states—the likelihood that two density matrices describe the same object. Our measure is motivated by two elementary requirements, which lead to a natural definition. We list some properties of this measure, and discuss its relation to the problem of combining two observers’ states of knowledge.

The quantum superposition principle induces a qualitative difference between classical and quantum states of knowledge. The state of a quantum system can be fully specified, yet not predict with certainty the outcome of a measurement—a state of affairs which has only the observers’ ignorance as classical analogue. In quantum mechanics, incomplete knowledge is represented by a mixed density matrix—though a mixed density matrix doesn’t necessarily reflect ignorance—which corresponds imperfectly to a classical distribution; the “quantum uncertainty” of pure states combines with the “classical uncertainty” of a distribution to yield an object which can be represented by different decompositions or realizations.

The fidelity of two quantum states \( \rho_A \) and \( \rho_B \),

\[
F(\rho_A, \rho_B) = \text{Tr} \left\{ \sqrt{\sqrt{\rho_A} \rho_B \sqrt{\rho_A}} \right\}
\]  

(or more precisely \( F^2 \)) measures the likelihood that various measurements made on the two states will obtain the same result. Thus, fidelity is a measure of similarity between states which does not distinguish between classical and quantum uncertainty.

In this letter, we introduce \textit{compatibility}, a measure similar to fidelity, but which compares two observers’ states of knowledge, not the results of the measurements which they could do. We want the compatibility to measure classical admixture, while treating different pure states as fundamentally different: if two observers claim to have complete knowledge of a system, their descriptions had better agree completely. Hence, a compatibility measure \( C(\rho_A, \rho_B) \) should satisfy the two following requirements:

1. When \( [\rho_A, \rho_B] = 0 \) (classical mixture) the compatibility should be equal to the fidelity.

2. The compatibility of incompatible states should be 0.

While our first requirement should be transparent, the second sounds tautological, and requires further explanation. Consider two observers (Alice and Bob) whose respective states of knowledge are described by \( \rho_A \) and \( \rho_B \). (Throughout this letter, we use subscript \( k \) to designate either \( A \) or \( B \).) Brun, Finkelstein, and Mermin [BFM02a] defined Alice’s and Bob’s descriptions to be \textit{compatible} if and only if they could be describing the same physical system. They then addressed the following question: under

\footnotesize{Caves, Fuchs, and Schack have recently challenged this statement [CFS02c]. The distinction between our studies leading to this disagreement can be summarized by “state of belief vs state of knowledge”.

6}
what conditions are $\rho_A$ and $\rho_B$ compatible? Their answer is quite simple: $\rho_A$ and $\rho_B$ are compatible if and only if the intersection of their supports, $S = S(\rho_A) \cap S(\rho_B)$, is nonempty. The support $S(\rho)$ of a density matrix $\rho$ is the complement of its null space $N(\rho)$; to obtain the projector $P_{S(\rho)}$ onto $S(\rho)$, diagonalize $\rho$ and replace each nonzero eigenvalue with 1. Thus, $\rho_A$ and $\rho_B$ are compatible if $P_{S(\rho_A)}P_{S(\rho_B)}$ has at least one unit eigenvalue. In other words, two states of knowledge are incompatible if between them they rule out all possible pure states.

With this definition, state $\rho_A = |0\rangle \langle 0|$ is compatible with both state $\rho_B = \epsilon |0\rangle \langle 0| + (1 - \epsilon) |1\rangle \langle 1|$ and state $\rho'_B = (1 - \epsilon) |0\rangle \langle 0| + \epsilon |1\rangle \langle 1|$ as long as $0 < \epsilon < 1$. Nevertheless as $\epsilon \to 0$, it is clear that the compatibility of $\rho_A$ and $\rho_B$ should vanish while that of $\rho_A$ and $\rho'_B$ should approach unity. The definition of [BFM02a] makes no distinction between these two cases and this is what originally motivated the present work.

Now that requirement 2 has been clarified, we can proceed with the definition of the compatibility measure.

**Definition C.5.1.** Let $\mathcal{B}_0(\mathcal{H})$ be the set of all density matrices on Hilbert space $\mathcal{H}$. For $\rho \in \mathcal{B}_0(\mathcal{H})$, define $\mathcal{P}(\rho)$ as the set of realizations of $\rho$:

$$\mathcal{P}(\rho) = \left\{ P : \int_{\mathcal{B}_0(\mathcal{H})} P(\sigma)\sigma d\sigma = \rho \right\} \quad (C.37)$$

where the $P$ are probability distributions over $\mathcal{B}_0(\mathcal{H})$. Then, the compatibility of $\rho_A$ and $\rho_B \in \mathcal{B}_0(\mathcal{H})$ is defined as

$$C(\rho_A, \rho_B) = \max_{P_A \in \mathcal{P}(\rho_A), P_B \in \mathcal{P}(\rho_B)} \int_{\mathcal{B}_0(\mathcal{H})} \sqrt{P_A(\sigma)P_B(\sigma)} d\sigma, \quad (C.38)$$

the integral representing the classical fidelity $F(P_A, P_B)$ (or statistical overlap) of two classical distributions $P_A$ and $P_B$.

**Lemma C.5.1.** All distributions $P \in \mathcal{P}(\rho)$ must vanish outside $\mathcal{B}_0(\rho)$: the set of density matrices with support restricted to $S(\rho)$ (this is a slightly abusive notation).

**Proof** Let $P(\sigma)$ be a realization of $\rho$. We can separate $\rho$ in two parts:

$$\rho = \int_{\mathcal{B}_0^\perp(\rho)} P_k(\sigma)\sigma d\sigma + \int_{\mathcal{B}_0(\rho)} P_k(\sigma)\sigma d\sigma = p\rho' + (1 - p)\rho'' \quad (C.39)$$
where \( \rho' \), by definition, has support on \( \mathcal{N}(\rho) \), \( \rho'' \) has support strictly on \( \mathcal{S}(\rho) \) and 
\[ p = \int_{\mathfrak{B}_0^+(\rho)} P_k(\sigma) \, d\sigma. \]
If \( p \neq 0 \), there exists \( \psi \in \mathcal{N}(\rho) \) such that \( \rho \) does not annihilate \( \psi \). This contradicts the definition of \( \mathcal{N}(\rho) \), so we conclude that \( p = 0 \) and therefore \( P \) is restricted to \( \mathfrak{B}_0(\rho) \).

**Theorem C.5.1.** Definition 1 satisfies both of our requirements.

**Proof**

1. If \( \rho_A \) commutes with \( \rho_B \), then they have orthogonal decompositions onto the same set of pure states: 
\[ \rho_A = \sum_i a_i |\phi_i\rangle \langle \phi_i|; \quad \rho_B = \sum_i b_i |\phi_i\rangle \langle \phi_i|. \]
Thus 
\[ C(\rho_A, \rho_B) \geq \sum_i \sqrt{a_i b_i} = F(\rho_A, \rho_B). \]
Later (see P4) we show that 
\[ C(\rho_A, \rho_B) \leq F(\rho_A, \rho_B); \]
therefore for commuting density matrices 
\[ C(\rho_A, \rho_B) = F(\rho_A, \rho_B). \]

2. If \( \rho_A \) and \( \rho_B \) are incompatible, their supports are disjoint, which implies that 
\[ P_A(\sigma) \text{ and } P_B(\sigma) \] are restricted to disjoint sets—implying that 
\[ C(\rho_A, \rho_B) = 0. \]

Note that this measure is not the only one which satisfies our two requirements. For example, define
\[ D_n(\rho_A, \rho_B) = Tr \left\{ \left( (\rho_A)^{1/2n}(\rho_B)^{1/n}(\rho_A)^{1/2n} \right)^{n/2} \right\}. \]

Clearly, 
\[ D_n(\rho_A, \rho_B) = F(\rho_A, \rho_B) \]
when \( n = 1 \) or for any \( n \) when \( |\rho_A, \rho_B| = 0 \), so it satisfies our first requirement. For the second requirement, notice that
\[ \lim_{n \to \infty} D_n(\rho_A, \rho_B) \leq \lim_{n \to \infty} Tr \left\{ \left[ P_{S(\rho_A)} P_{S(\rho_B)} \right]^{n/2} \right\}, \]
which is 0 if \( P_{S(\rho_B)} P_{S(\rho_B)} \) has no unit eigenvalue, i.e., if \( \rho_A \) and \( \rho_B \) are incompatible. Therefore 
\[ D(\rho_A, \rho_B) = \lim_{n \to \infty} D_n(\rho_A, \rho_B) \]
is a valid measure of compatibility.

Definition C.5.1 can also be generalized to
\[ E_\alpha(\rho_A, \rho_B) = \max_{P_A \in \mathcal{P}(\rho_A)} \int_{\mathfrak{B}_0(\mathcal{H})} [P_A(\sigma)]^{\alpha} [P_B(\sigma)]^{1-\alpha} \, d\sigma \]
\[ 0 < \alpha < 1 \]
which is the Rényi overlap of \( P_A \) and \( P_B \), the fidelity corresponding to the special case \( \alpha = 1/2 \). This definition allows for an asymmetry between Alice and Bob which can be useful when one of the participant is more trustworthy than the other.

Although these alternative definitions offers some interesting features, we shall concentrate on Definition C.5.1 in the following. (Superscript \( D \) and \( E \) indicates that the results also hold for measure \( D(\rho_A, \rho_B) \) and \( E_\alpha(\rho_A, \rho_B) \) respectively, the proofs are given for \( C(\rho_A, \rho_B) \) only.)
Theorem C.5.2. \( E \) To compute the compatibility of two states, it is sufficient to maximize over pure state realizations. In other words

\[
C(\rho_A, \rho_B) = \max_{Q_A \in \mathcal{Q}(\rho_A)} \int_{\mathcal{B}_0(\mathcal{H})} \sqrt{Q_A(\psi)Q_B(\psi)} d\psi
\]

where \( \mathcal{B}_0(\mathcal{H}) \) is the set of all pure states in \( \mathcal{H} \) and \( \mathcal{Q}(\rho) \) is the set of pure state realizations of \( \rho \):

\[
\mathcal{Q}(\rho) = \left\{ Q : \int_{\mathcal{B}_0(\mathcal{H})} Q(\psi) |\psi\rangle \langle \psi| d\psi = \rho \right\},
\]

\( Q \) are probabilities distributions on \( \mathcal{B}_0(\mathcal{H}) \).

Proof\ Choose a standard pure state decomposition for \( \sigma \in \mathcal{B}_0(\mathcal{H}), \sigma = \int_{\mathcal{B}_0(\mathcal{H})} f_{\sigma}(\psi)|\psi\rangle \langle \psi| d\psi \) (e.g., eigendecomposition). Then

\[
\int_{\mathcal{B}_0(\mathcal{H})} \sqrt{P_A(\sigma)P_B(\sigma)} d\sigma 
\]

\[
= \int_{\mathcal{B}_0(\mathcal{H})} \int_{\mathcal{B}_0(\mathcal{H})} \sqrt{P_A(\sigma)f_{\sigma}(\psi)P_B(\sigma)f_{\sigma}(\psi)} d\sigma d\psi 
\]

\[
\leq \int_{\mathcal{B}_0(\mathcal{H})} \sqrt{Q_A(\psi)Q_B(\psi)} d\psi
\]

since fidelity can only increase under the marginalization \( Q_k(\psi) = \int_{\mathcal{B}_0(\mathcal{H})} P_k(\sigma)f_{\sigma}(\psi) d\sigma \).

Theorem C.5.3. When one of the two states is pure (say \( \rho_B \)), \( C(\rho_A, \rho_B) = \sqrt{p} \) where \( p \) is given by

\[
p = \min_{q \in [0,1]} \left\{ q : \det \left\{ \rho_A - q\rho_B \right\} = 0 \right\}
\]

if \( \rho_B \) lies within \( S(\rho_A) \) and \( p = 0 \) otherwise.

Proof\ There is a unique realization for \( \rho_B \): \( P_B(\sigma) = \delta(\sigma - \rho_B) \). The maximum value of \( q \) for which we can write \( \rho_A = q\rho_B + (1-q)\sigma \) (with \( \sigma \) a valid density matrix) is \( p \). The result follows.

Theorem C.5.4. \( E \) Any local maximum of \( F(P_A, P_B) \) over \( \mathcal{P}(\rho_A) \otimes \mathcal{P}(\rho_B) \) is a global maximum.

Proof\ Fidelity is a concave function: \( F(\lambda P_A + [1-\lambda]P_A', P_B) \geq \lambda F(P_A, P_B) + [1-\lambda]F(P_A', P_B) \). The sets \( \mathcal{P}(\rho_A) \) and \( \mathcal{P}(\rho_B) \) are convex: any convex combinations of valid probability
distributions of mean $\rho$ is also a valid probability distribution with mean $\rho$. The result follows automatically.

We now give a list of properties of the compatibility measure.

**P1** $D$ $C(\rho_A, \rho_B)$ is symmetric.

**P2** $DE$ Compatibility is invariant under unitary transformation: $C(U\rho_AU^\dagger, U\rho_BU^\dagger) = C(\rho_A, \rho_B)$.

**P3** $DE$ For pure states $C(\psi_A, \psi_B) = 1$ if and only if $|\langle \psi_A | \psi_B \rangle|^2 = 1$ and 0 otherwise.

**P4** $D$ (Upper bound) $C(\rho_A, \rho_C) \leq F(\rho_A, \rho_B)$.

**P5** $DE$ $F(\rho_A, \rho_B) = 0 \Rightarrow C(\rho_A, \rho_B) = 0$ and $F(\rho_A, \rho_B) = 1 \Leftrightarrow C(\rho_A, \rho_B) = 1 \Leftrightarrow \rho_A = \rho_B$.

**P6** (Lower bound) $C(\rho_A, \rho_B) \geq r\sqrt{\epsilon_A \epsilon_B}$ where $\epsilon_k$ is the greatest value of $q$ for which one can write $\rho_k = \frac{q}{r}P_S + (1-q)\sigma$ with $\sigma$ being a valid density matrix, see (eq.C.47), and $r = Tr\{P_S\}$ is the dimension of $S = S(\rho_A) \cap S(\rho_B)$. (For compatible states, $\epsilon_k \geq \lambda^0_k$, the smallest nonzero eigenvalue of $\rho_k$.)

**P7** $E$ (Multiplicativity) $C(\rho_A \otimes \rho'_A, \rho_B \otimes \rho'_B) \geq C(\rho_A, \rho_B)C(\rho'_A, \rho'_B)$.

**Proofs**

P1, P2, and P3 are straightforward from Definition C.5.1.

P4: Assume that $Q_k(\psi)$ are the optimal distributions given by Theorem C.5.2. We choose $\vec{x} \in \mathbb{R}^{(2N-2)}$ (where $N$ is the dimension of $\mathcal{H}$) as a parameterization for $\mathfrak{B}_1(\mathcal{H})$: $\psi = \psi(\vec{x})$, and construct the purifications

$$|\Psi_k\rangle = \int \sqrt{Q_k(\psi(\vec{x}))}|\psi(\vec{x})\rangle \otimes |\vec{x}\rangle \ d\vec{x} \quad (C.48)$$

where $\vec{x}$ is now treated as a quantum continuous variable $\langle \vec{x} | \vec{x}' \rangle = \delta(\vec{x} - \vec{x}')$ (e.g. position of a particle in a $N$-dimensional box). Then $C(\rho_A, \rho_B) = \langle \Psi_A | \Psi_B \rangle \leq F(\rho_A, \rho_B)$ since the fidelity is the maximum of this quantity over all purifications.

This proof introduces an interesting distinction between fidelity and compatibility. Fidelity is the optimal inner product between all purifications of $\rho_A$ and $\rho_B$. On the other hand, compatibility involves purifications of a very special kind (eq.C.48). All that is needed to transform compatibility into fidelity is to replace (eq.C.48) by

$$|\Psi_A\rangle = \int \sqrt{Q_A(\psi(\vec{x}))}|\psi(\vec{x})\rangle \otimes U_A|\vec{x}\rangle \ d\vec{x}$$

$$|\Psi_B\rangle = \int \sqrt{Q_B(\psi(\vec{x}))}|\psi(\vec{x})\rangle \otimes U_B|\vec{x}\rangle \ d\vec{x} \quad (C.49)$$
C.5. Compatibility of quantum states

for arbitrary unitary operators \( U_A \) and \( U_B \).

P5 follows from \( F(\rho_A, \rho_B) = 1 \iff \rho_A = \rho_B \), requirement 1, and P4.

P6: We can choose a distribution where \( \rho_k \) has probability \( r_{\epsilon_k} \) at the point \( \sigma = P_S / r \).

P7: The product of the optimal distributions for \( C(\rho_A, \rho_B) \) and \( C(\rho'_A, \rho'_B) \) are valid distributions over the combined Hilbert space but might not be optimal. We do not know if this inequality can be reduced to an equality. In other words, it is possible that the optimal distribution for \( \rho_A \otimes \rho'_A \) and \( \rho_B \otimes \rho'_B \) involve non product states.

It is worth mentioning that no smooth function of the compatibility satisfying \( f(C) = 1 \iff C = 0 \) and \( f(C) = 0 \iff C = 1 \) can be used to build a metric on \( \mathfrak{B}_0(\mathcal{H}) \). This is best illustrated by the following 2-dimensional example. Assume states \( \rho_+ \) and \( \rho_- \) are pure, derived from \( |\psi_\pm\rangle = \cos \epsilon |0\rangle \pm \sin \epsilon |1\rangle \), and \( \rho_0 = (1 - \epsilon^2)|0\rangle \langle 0| + \epsilon |1\rangle \langle 1| \) where \( \epsilon \rightarrow 0 \). One can easily verify that \( C(\rho_+, \rho_-) = 0 \) and \( C(\rho_+, \rho_0) = C(\rho_-, \rho_0) = 1 - \mathcal{O}(\epsilon) \) so \( f(C(\rho_+, \rho_-)) = 1 > f(C(\rho_+, \rho_0)) + f(C(\rho_-, \rho_0)) \rightarrow 0 \) as \( \epsilon \rightarrow 0 \). This is in contrast with classical distributions: when \( [\rho_A, \rho_B] = 0 \), \( \cos^{-1} F(\sqrt{\rho_A \rho_B}) \) is a valid distance measure [Fuc96a].

**Measurements**

Suppose that Alice and Bob acquire their knowledge of \( \rho_A \) and \( \rho_B \) through measurement. These states will always be compatible: incompatible knowledge acquired through measurement would indicate an inconsistency in quantum theory. For example, they can each be given many copies of a quantum system in state \( \rho \) of which they initially have no knowledge except the dimension. They carry out independent measurements on those copies and, with the help of Bayesian rules, update their description of the system (see [SBC01a] and references therein). As mentioned earlier, their descriptions will always be compatible. Nevertheless, a low compatibility could result as a consequence of one of the following situations: i) they were given copies of different states, i.e. the promise of identical systems was broken; ii) their measurement apparatus are miscalibrated; or iii) they are in a very improbable branch of the Universe.

\footnote{Incompatible knowledge could emerge as a consequence of the finite accuracy of the measurement apparatus: nevertheless, such limitations should be taken into account in the state estimation.}
These eventualities cannot be detected by the fidelity of $\rho_A$ and $\rho_B$. For example, suppose that, for a 2-level system,

\begin{align*}
  \rho_A &= (1 - \epsilon)|0\rangle\langle 0| + \frac{\epsilon}{2} \mathbb{I} \\
  \rho_B &= (1 - \epsilon)|+\rangle\langle +| + \frac{\epsilon}{2} \mathbb{I},
\end{align*}

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. As the observers’ knowledge becomes more and more accurate ($\epsilon \to 0$), the compatibility goes to 0, indicating one of the three situations listed above. On the other hand, fidelity saturates at $F^2 = 1/2$, which is the same as if both Alice and Bob had a vague knowledge of the state, e.g.

\begin{align*}
  \rho_A &= (\frac{1}{2} + a)|0\rangle\langle 0| + (\frac{1}{2} - a)|1\rangle\langle 1| \\
  \rho_B &= (\frac{1}{2} - a)|0\rangle\langle 0| + (\frac{1}{2} + a)|1\rangle\langle 1|,
\end{align*}

with $a = \sqrt{2}/4$. This clearly illustrates the fact that fidelity makes no distinction between classical and quantum uncertainty.

**Combining knowledge**

Now, suppose Alice and Bob want to pool their information. If $C(\rho_A, \rho_B) = 0$ (which cannot result from measurement), their “knowledge” is contradictory. When $C(\rho_A, \rho_B) > 0$, however, they can combine their states of knowledge to get a new density matrix $\rho_{AB}$. This issue has recently been studied by Jacobs [Jac02a] but with the only conclusion that $\rho_{AB}$ should lie in $S(\rho_A) \cap S(\rho_B)$.

We propose that the state obtained from combining two states of knowledge should be the one which is maximally compatible with both of them. This requires a definition of three-way compatibility:

\begin{equation}
  C(\rho_A, \rho_B, \rho_C) = \max_{\rho} \int_{\mathcal{M}_2(\mathcal{H})} \sqrt[3]{P_A(\sigma)P_B(\sigma)P_C(\sigma)} d\sigma.
\end{equation}

Hence, our rule for combining states of knowledge reads

\begin{equation}
  \rho_{AB} = \text{Argument} \left( \max_\rho C(\rho_A, \rho_B, \rho) \right);
\end{equation}

in the eventuality that the maximum over $\rho$ is not unique, one can discriminate with a maximum entropy $S(\rho)$ criteria which is well motivated in the current context. For any
fixed $P_A$ and $P_B$, the $P_C$ that optimizes (eq.C.53) is proportional to the geometric average of $P_A$ and $P_B$. Therefore, defining $\tilde{P}_A$ and $\tilde{P}_B$ as the distributions which optimized equation (C.38), we get

$$\rho_{AB} = \int_{\mathcal{M}(\mathcal{H})} P_{AB}(\sigma) \sigma \, d\sigma \quad (C.54)$$

where $P_{AB} = \sqrt{\tilde{P}_A \tilde{P}_B}/C(\rho_A, \rho_B)$. Furthermore, there is a simple relation between the optimal three-way compatibility and the compatibility of the two original descriptions: $C(\rho_A, \rho_B, \rho_{AB})^3 = C(\rho_A, \rho_B)^2$.

**Knowledge**

Knowledge of a quantum system can take many forms; as Bennett expresses it,

It is possible to *know* or *possess* a quantum state in infinitely many physically inequivalent ways, ranging from complete classical knowledge, through possession of a single specimen of the state, to weaker and less compactly embodiable forms such as the ability to simulate the outcome of a single POVM measurement on the state. [Ben01a]

The compatibility measurement of (eq.C.38) is meaningful when we consider classical description of the quantum states; the quantum fidelity (eq.C.36) corresponds to a situation where single specimens of the quantum states are available (respectively “knowledge of the quantum” and “quantum knowledge”). One can define compatibility measurements according to the *type of knowledge* one is dealing with. For example, we can define the compatibility between a state $\rho$ and an ensemble $\{q_j, \sigma_j\}$ as $\max_{P(\rho)} F(P, Q)$ where $Q(\sigma) = \sum_j q_j \delta(\sigma - \sigma_j)$. While the pure state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is compatible with the ensemble $E_1 = \{|1, p\rangle|0\rangle + (1-p)|1\rangle|1\rangle\}$, it is incompatible with the ensemble $E_2 = \{|p, |0\rangle|0\rangle, (1-p), |1\rangle|1\rangle\}$, even if they are realizations of the same state.

An ensemble embodies more knowledge than its associated (average) state. In our prescription for combining knowledge, we have assumed that all of Alice’s and Bob’s knowledge was encapsulated in their respective density matrices. Note that all knowledge can be represented in this form by including ancillary systems [e.g. eq.(C.48)].

Suppose, instead, that both Alice’s and Bob’s states of knowledge are represented by the ensemble $E_1$. Obviously, their combined density matrix should be $\rho_{AB1} =$
$p|0\rangle\langle 0| + (1 - p)|1\rangle\langle 1|$. On the other hand, when both their states of knowledge are $E_2$, Bayesian rules would suggest that their combined state should be $\rho_{AB2} = p^2|0\rangle\langle 0| + (1 - p)^2|1\rangle\langle 1|$ (with proper normalization)—but this assumes that their knowledge was acquired independently [Jac02a]. If their knowledge came from a redundant source, the Bayesian rule would then yield state $\rho_{AB1}$, as would our prescription.

Hence, this illustrates that our rule for combining states of knowledge assumes no more information than what is encapsulated in the density matrices. Furthermore, it can quite simply be adapted to different forms of knowledge, either through the use of ancillary systems or of generalized compatibility measures.

Acknowledgements—The authors would like to acknowledge Howard Barnum, Kurt Jacobs, Harold Ollivier, and Wojciech Zurek for discussions on this subject. RBK would also like to thank Todd Brun for discussions and inspiration.
C.6. Noiseless Subsystems for Collective Rotation Channels in Quantum Information Theory†

John A. Holbrook1, David W. Kribs1,2,3, Raymond Laflamme2,3 and David Poulin2,3

1Department of Mathematics and Statistics, University of Guelph, Guelph, ON, CANADA N1G 2W1.
2Institute for Quantum Computing, University of Waterloo, Waterloo, ON, CANADA N2L 3G1.
3Perimeter Institute for Theoretical Physics, 35 King St. North, Waterloo, ON, CANADA N2J 2W9.

Abstract: Collective rotation channels are a fundamental class of channels in quantum computing and quantum information theory. The commutant of the noise operators for such a channel is a $C^*$-algebra which is equal to the set of fixed points for the channel. Finding the precise spatial structure of the commutant algebra for a set of noise operators associated with a channel is a core problem in quantum error prevention. We draw on methods of operator algebras, quantum mechanics and combinatorics to explicitly determine the structure of the commutant for the class of collective rotation channels.

†Accepted for publication in Integral Equations & Operator Theory.
Introduction

Quantum information theory provides the underlying mathematical formalism for quantum computing and is an interesting field of research in its own right [NC00a]. While quantum computing and communication promise far reaching applications [Bro99a, Joh03a, Nie02a], there are numerous technical and theoretical difficulties that must be overcome. Of particular interest is the study of quantum error correction and error prevention methods. In classical computing, the types of errors that can occur are very limited. On the other hand, the fragile nature of quantum systems shows that in quantum computing there is a much richer variety of potential errors. Fortunately, methods of quantum error correction have recently been developed showing, in principle, that these difficulties may be overcome (see [AB98a, Got02b, Kit97d, KLA+02a, KLZ98a, Pre98a] for an introduction to the subject).

Central to quantum information theory is the analysis of quantum channels [NC00a]. Mathematically, a quantum channel is given by a completely positive trace preserving map which acts on the set of operators on a finite dimensional Hilbert space. Every channel has a family of noise operators that determine the map in a natural way. One of the most promising methods of passive quantum error correction, recently developed by the third author and others [DG97c, FVP+03a, HKL04a, KLA+02a, KLV00a, LCW98a, ZR97c], is called the noiseless subsystem method. Given a quantum channel, the basic tenet of this method is to use the structure of the operator algebra defined by the commutant of the associated noise operators to prepare initial quantum states which are immune to the noise of the channel. Thus it is a fundamental problem in quantum error correction to find the structure of this ‘noise commutant’. However, let us emphasize that it is the precise spatial structure of this algebra that must be identified. This point is clarified in the discussion of the next section.

An important test class for the noiseless subsystem method and other quantum error correction methods is the class of collective rotation channels [BRS03a, BGL+03a, dF00a, FVP+03a, HKL04a, KBLW01a, KLV00a, VKL01a, VFP+01a, ZL03a, Zan01b, Zar03a]. This class has its roots in the depths of quantum mechanics, specifically in the study of angular momentum at the atomic level (see for example [CTDL77a]). A realistic physical situation where these channels arise occurs when quantum information, encoded as light pulses, is transmitted through an optical fibre [FVP+03a, VFP+01a]. In such a situation, the fibre can produce a ‘collective rotation’ of the information.
In [BS98b, Kri03a] it was shown that when a channel is unital, which is the case for collective rotation channels, the noise commutant is a finite dimensional $C^*$-algebra which is equal to the fixed point set for the channel. Based on operator algebra techniques, the paper [HKL04a] derives an algorithm for computing the commutant structure in the most general setting. However, for particular cases such as the channels considered here, the required computations can become unwieldy.

In this paper, based on the theory of operator algebras and quantum mechanics, we compute the noise commutant structure for the class of collective rotation channels. We provide a constructive proof which yields a simple visual interpretation based on Pascal’s triangle. This result may also be derived from well-known representation theory techniques; however, our direct operator theory cum quantum mechanical approach is novel and offers a new perspective on the general problem.

The next section contains a brief review of the material we require from the theories of operator algebras and quantum information. In the third section we define the collective rotation channels and establish some basic properties. The fourth section contains the commutant structure theorem for the ‘qubit’ case (Theorem C.6.1). Finally, we conclude the paper by presenting a commutant structure theorem for more general classes of collective rotation channels (Theorem C.6.2).

One final comment. A study of the quantum information and quantum computing literature reveals that many techniques from operator theory and operator algebras have been, or could be, used to build mathematical foundations for the physical theories in these areas. An idea we wish to promote is that there is a wealth of interesting mathematics to be found in this young field.

**Background**

Motivated by the postulates of quantum mechanics, an assumption typically made in quantum information theory is that every quantum operation on a closed quantum system is reversible [CTDL77a, NC00a]. Mathematically, this statement means that the operation is described by unitary evolution; in other words, there is a unitary operator $U$ on a Hilbert space $\mathcal{H}$ such that the operation is implemented by the conjugation map $\rho \mapsto U\rho U^\dagger$ where $\rho$ is an operator on $\mathcal{H}$. (Here we use the physics convention $U^\dagger$ for conjugate transpose.) Often $\rho$ is a density operator, a positive operator with trace equal to one, that corresponds to the initial state of the quantum system of interest, but in
our analysis there is no loss of generality in considering evolution of any operator under the quantum operation. Further note that $U$ can be restricted to the special unitary group $SU(N)$, where $N = \dim(\mathcal{H})$, since the evolution $\rho \mapsto U\rho U^\dagger$ is unaffected by the multiplication of $U$ by a complex phase.

Of course, in practice a given quantum operation will not be reversible because of interactions with the environment. In this more realistic setting the quantum operation is regarded as acting on a closed quantum system that contains the original as a subsystem. The mathematical formalism for this is given by completely positive maps [Cho75a, Kra71a, Pau86a, Pau02a] and the Stinespring dilation theorem [Sti55a]. Specifically, every quantum operation is represented mathematically by a quantum channel.

Given a (finite dimensional) Hilbert space $\mathcal{H}$, a quantum channel is a map $\mathcal{E}$ which acts on the set $\mathcal{B}(\mathcal{H})$ of all operators on $\mathcal{H}$ and is completely positive and trace preserving. For each channel $\mathcal{E}$ there is a set of (non-unique) noise operators [Cho75a, Kra71a] $\{A_1, \ldots, A_n\}$ that determine the map through the equation

$$\mathcal{E}(\rho) = \sum_{k=1}^{n} A_k \rho A_k^\dagger \quad \text{for} \quad \rho \in \mathcal{B}(\mathcal{H}). \quad (C.55)$$

Physically, the associated quantum operation can be regarded as determined by a compression of the Stinespring unitary dilation, that acts on a larger closed quantum system, of the completely positive map (C.55). Trace preservation is equivalent to the noise operators satisfying the equation

$$\sum_{k=1}^{n} A_k^\dagger A_k = \mathbb{1},$$

where $\mathbb{1}$ is the identity operator on $\mathcal{H}$. The channel is unital if also,

$$\mathcal{E}(\mathbb{1}) = \sum_{k=1}^{n} A_k A_k^\dagger = \mathbb{1}.$$  

Let $\text{Fix}(\mathcal{E}) = \{\rho \in \mathcal{B}(\mathcal{H}) : \mathcal{E}(\rho) = \rho\}$ be the fixed point set for $\mathcal{E}$ and let $\mathcal{A}$ be the algebra generated by $A_1, \ldots, A_n$ from (C.55). This is called the interaction algebra in quantum information theory [KLV00a]. In general, $\text{Fix}(\mathcal{E})$ is just a $\dagger$-closed subspace of $\mathcal{B}(\mathcal{H})$, but it was shown (independently) in [BS98b] and [Kri03a] that, in the case of a unital channel $\mathcal{E}$, the so-called noise commutant $\mathcal{A}' = \{\rho \in \mathcal{B}(\mathcal{H}) : \rho A_k = A_k \rho, \ k = 1, \ldots, n\}$ coincides with this set:

$$\text{Fix}(\mathcal{E}) = \mathcal{A}'.$$
In particular, $\text{Fix}(\mathcal{E}) = \mathcal{A}'$ is a $\dagger$-closed operator algebra (a finite dimensional C*-algebra [Arv76a, Dav96a]). Further, the von Neumann double commutant theorem shows how the algebra $\mathcal{A} = \mathcal{A}'' = \text{Fix}(\mathcal{E})'$ only depends on the channel; that is, it is independent of the choice of noise operators that determine the channel as in (C.55).

It is a fundamental result in finite dimensional C*-algebra theory [Arv76a, Dav96a, Tak79a] that every such algebra is unitarily equivalent to an orthogonal direct sum of ‘ampliated’ full matrix algebras; i.e., there is a unitary operator $U$ such that

$$U\mathcal{A}U^\dagger = \bigoplus_{k=1}^{d} (\mathbb{1}_{m_k} \otimes \mathcal{M}_{n_k}),$$

where $\mathcal{M}_{n_k}$ is the full matrix operator algebra $\mathcal{B}(\mathbb{C}^{n_k})$. The numbers $m_k$ in this decomposition correspond to the multiplicities in the C*-algebra representation that gives $\mathcal{A}$. With this form for $\mathcal{A}$ given, the structure of the commutant up to unitary equivalence is easily computed by

$$\mathcal{A}' \cong \bigoplus_{k=1}^{d} (\mathcal{M}_{m_k} \otimes \mathbb{1}_{n_k}).$$  \hspace{1cm} (C.56)

(See [FVP+03a, HKL04a, KBLW01a, VKL01a, ZL03a, Zan01b] for more detailed discussions in connection with quantum information theory.) The projections onto the $m_kn_k$ dimensional subspaces associated with the summands in this decomposition are the minimal central projections for $\mathcal{A}$ (and $\mathcal{A}'$). Each such projection is the sum of $n_k$ rank $m_k$ projections which are minimal reducing for $\mathcal{A}'$. We describe this situation by saying these $n_k$ projections are ‘linked’ inside $\mathcal{A}'$.

On the other hand, for a given quantum channel $\mathcal{E}$ with noise operators $\{A_k\}$, the noise commutant $\mathcal{A}'$ plays a significant role in quantum error prevention. The structure of this commutant can be used to prepare density operators, which encode the state of a given quantum system, for use in the noiseless subsystem method of error correction. This is a passive method of quantum error correction, in the sense that such operators will remain immune to the effects of the noise operators, or ‘errors’ of the channel, without active intervention. But more is true. The algebra structure discussed above shows that quantum operations may be performed on such a subsystem, provided the corresponding unitary operators belong to the commutant. Keeping in mind our earlier description of an optical fibre, the reader can imagine a situation where it is desirable
to transfer quantum information through the fibre such that the information remains immune to the errors of collective rotations produced by the fibre.

As discussed above, understanding the structure of $A'$ is of fundamental importance in quantum error correction. But there is an operator algebra subtlety here which is worth emphasizing. Typically, it is not feasible in this setting to wash away the particular representation which gives $A'$ with $*$-isomorphisms, unitary equivalences, etc., as is the custom in operator algebra theory. Indeed, by the very nature of the problems, it is the precise spatial algebra structure of $A'$ which must be identified, ampliations included.

The basic problem of computing $A'$ was addressed in [HKL04a] for the general case of a unital quantum channel. We also mention more recent work [Zar03a] where computer algorithms have been written for this and other related purposes. However, in particular cases, such as the class of channels considered in this paper, a more delicate approach based on special properties of the class can be exploited to find this structure more directly and efficiently.

**Collective Rotation Channels**

Let $\{|-\frac{1}{2}\rangle, |\frac{1}{2}\rangle\}$ be a fixed orthonormal basis for 2-dimensional Hilbert space $\mathcal{H}_2 = \mathbb{C}^2$, corresponding to the classical base states in a two level quantum system (e.g. the ground and excited states of an electron in a Hydrogen atom). Note that such a basis is usually written as $\{|0\rangle, |1\rangle\}$, but the $-\frac{1}{2}, \frac{1}{2}$ notation is more convenient for the combinatorics below. A ‘qubit’ or ‘quantum bit’ of information is given by a unit vector $|\psi\rangle = \alpha |-\frac{1}{2}\rangle + \beta |\frac{1}{2}\rangle$ inside $\mathcal{H}_2$. When both $\alpha$ and $\beta$ are non-zero, $|\psi\rangle$ is said to be a *superposition* of $|-\frac{1}{2}\rangle$ and $|\frac{1}{2}\rangle$.

We shall make use of the abbreviated form from quantum mechanics for the associated standard orthonormal basis for $\mathcal{H}_{2^n} = (\mathbb{C}^2)^{\otimes n} \simeq \mathbb{C}^{2^n}$. For instance, the basis for $\mathcal{H}_4$ is given by

$$\{|ij\rangle : i,j \in \{-\frac{1}{2}, \frac{1}{2}\}\}$$

where $|ij\rangle$ is the vector tensor product $|ij\rangle \equiv |i\rangle |j\rangle \equiv |i\rangle \otimes |j\rangle$.

Let $\{\sigma_x, \sigma_y, \sigma_z\}$ be the spin-1/2 Pauli matrices given by

$$\sigma_x = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
Further let $\mathbb{I}_2$ be the $2 \times 2$ identity matrix. We shall regard these as the matrix representations for operators acting on $\mathcal{H}_2$ with respect to $\{|\frac{1}{2}\rangle, |\frac{1}{2}\rangle\}$. The Pauli matrices satisfy the following commutation relations:

1. $[\sigma_x, \sigma_y] = i\sigma_z$
2. $[\sigma_z, \sigma_x] = i\sigma_y$
3. $[\sigma_y, \sigma_z] = i\sigma_x$.

These are the canonical commutation relations which define the Lie algebra $su(2)$, given by the linear space $r_x \sigma_x + r_y \sigma_y + r_z \sigma_z = \vec{r} \cdot \vec{\sigma}$ with $(r_x, r_y, r_z) \in \mathbb{R}$. This algebra is the generator of the Lie group $SU(2)$ as the manifold of $2 \times 2$ unitary matrices with unit determinant and is isomorphic to the manifold $\{\exp(-i2\pi\vec{r} \cdot \vec{\sigma}) : ||\vec{r}|| \leq 1\}$. The group $SU(2)$ is referred to as the rotation group as it is homeomorphic to $O(3)$, the rotational group in three-dimensional space. Note that a rotation is the most general transformation which can be performed on a closed two-dimensional quantum system.

Now let $n \geq 1$ be a fixed positive integer. Define operators $\{J_z^{(k)} : 1 \leq k \leq n\}$ on $\mathcal{H}_{2^n}$ by

$$J_z^{(1)} = \sigma_z \otimes (\mathbb{I}_2)^{(n-1)}, \quad J_z^{(2)} = \mathbb{I}_2 \otimes \sigma_z \otimes (\mathbb{I}_2)^{(n-2)}, \quad \ldots,$$

where we use the standard ordering $(a_{kl}B)_{kl}$ for the tensor product of matrices $A \otimes B$. Similarly define $\{J_x^{(k)}, J_y^{(k)} : 1 \leq k \leq n\}$. Then the collective rotation generators $\{J_x, J_y, J_z\}$ are given by

$$J_x = \sum_{k=1}^{n} J_x^{(k)}, \quad J_y = \sum_{k=1}^{n} J_y^{(k)}, \quad J_z = \sum_{k=1}^{n} J_z^{(k)}.$$

Let us set down the fundamental commutation relations satisfied by these operators [CTDL77a].

**Proposition C.6.1.** The following relations hold for $\{J_x, J_y, J_z\}$:

1. $[J_x, J_y] = iJ_z$
2. $[J_z, J_x] = iJ_y$
3. $[J_y, J_z] = iJ_x$.

**Proof.** These identities easily follow from corresponding equations for $J_z^{(k)}, J_y^{(k)}, J_z^{(k)}$, with $1 \leq k \leq n$, which are simple consequences of the commutation relations (1), (2), (3) satisfied by the spin-1/2 Pauli matrices.
**Note C.6.1.** Observe that Proposition C.6.1 shows \( \{J_x, J_y, J_z\} \) determine a \( 2^n \)-dimensional representation of \( su(2) \).

In what follows, much of the analysis will be focused on the operators

\[
J_+ = J_x + iJ_y \quad \text{and} \quad J_- = J_x - iJ_y = J^\dagger_+.
\]

We shall also consider the so-called \( J \)-total operator \( J^2 \) defined by

\[
J^2 = J^2_x + J^2_y + J^2_z.
\]

The \( J^2 \) notation comes from the fact that this operator is conventionally defined as a vector product of matrices [CTDL77a].

Intuitively, the collective rotation channel is one where every qubit undergoes the same unknown rotation. Let us formalize this notion. Consider a channel \( \mathcal{E}_{U \otimes n} : \mathcal{B}(\mathcal{H}_2^\otimes n) \to \mathcal{B}(\mathcal{H}_2^\otimes n) \) defined as \( \mathcal{E}_{U \otimes n}(T) = (U \otimes n)^T \) for \( U \in SU(2) \). This is a collective rotation of \( n \) qubits which can also be written \( \mathcal{E}_{U \otimes n}(T) = \exp(-i2\pi \vec{r} \cdot \vec{J})T \exp(i2\pi \vec{r} \cdot \vec{J}) \), where \( \vec{r} \cdot \vec{J} = r_x J_x + r_y J_y + r_z J_z \) and \( U = \exp(-i2\pi \vec{r} \cdot \vec{\sigma}) \). Hence the appellation **collective rotation generators**.

But here, the specific rotation \( U \) is unknown and chosen at random over \( SU(2) \) according to a given probability density \( P(\vec{r}) \), for instance the distribution corresponding to Haar measure on \( SU(2) \). Then, the \( n \)-qubit collective rotation channel (relative to \( P(\vec{r}) \)) can be written as

\[
\mathcal{E}_n(T) = \int_{\{||\vec{r}||\leq 1\}} \exp(-i2\pi \vec{r} \cdot \vec{J})T \exp(i2\pi \vec{r} \cdot \vec{J})P(\vec{r})d\vec{r}; \tag{C.57}
\]

it is a weighted average of all collective rotations. By the symmetry of the integrated region, it can be shown that this unital channel can also be expressed in a more conventional form,

\[
\mathcal{E}_n(T) = E_x T E_x^\dagger + E_y T E_y^\dagger + E_z T E_z^\dagger, \tag{C.58}
\]

where the noise operators are defined as

\[
E_x = \frac{1}{\sqrt{3}} \exp(i\theta_x J_x), \quad E_y = \frac{1}{\sqrt{3}} \exp(i\theta_y J_y), \quad E_z = \frac{1}{\sqrt{3}} \exp(i\theta_z J_z),
\]

and \( \theta_k, k = x, y, z \), are angles determined by the probability distribution \( P(\vec{r}) \) [CTDL77a].
It is not hard to see that our analysis is independent of the particular choices for these angles, provided each $\theta_k$ is non-zero. Indeed, through a standard functional calculus argument from operator algebra, it can be seen that the interaction algebras generated by the $J_k$ and $E_k$ coincide, whatever the choice of $\theta_k$;

$A_n \equiv \text{Alg}\{J_x, J_y, J_z\} = \text{Alg}\{J_+, J_-, J_z\} = \text{Alg}\{E_x, E_y, E_z\}$. \hspace{1cm} (C.59)

In particular, as observed in [HKL04a], the fixed point set of this channel is determined by the original rotation generators.

**Proposition C.6.2.** Let $n \geq 1$ be a positive integer. Then

$$\text{Fix}(\mathcal{E}_n) = A'_n = \{E_x, E_y, E_z\}' = \{J_x, J_y, J_z\}'.$$  

Further, this commutant may be computed by considering the joint commutant of any pair from $\{J_x, J_y, J_z\}$.

**Commutant Structure Theorem**

Given a positive integer $n \geq 1$, let $\Delta_n$ denote the graph of $\binom{n}{2}$; that is, the graph of the $n$th line in Pascal’s triangle. (See the example below for a pictorial perspective.) Let

$$\mathcal{J}_n = \left\{ \begin{array}{ll} \{0, 1, \ldots, \frac{n}{2}\} & \text{if } n \text{ is even} \\ \{\frac{1}{2}, \frac{3}{2}, \ldots, \frac{n}{2}\} & \text{if } n \text{ is odd} \end{array} \right.$$  

Observe that the cardinality of $\mathcal{J}_n$ is equal to the number of steps up one side of $\Delta_n$.

**Theorem C.6.1.** Let $\mathcal{E}_n$ be the collective rotation channel for a fixed positive integer $n \geq 1$. Then

$$\text{Fix}(\mathcal{E}_n) = A'_n = \bigoplus_{j \in \mathcal{J}_n} A'_{(j)},$$  

where $A'_{(j)}$ is a $C^*$-subalgebra of $A'_n$ given, up to unitary equivalence, by

$$A'_{(j)} \simeq M_{p_j} \otimes 1_{q_j} \quad \text{for} \quad j \in \mathcal{J}_n,$$

with $p_{\frac{n}{2}} = 1$ and for $j \in \mathcal{J}_n$, $j < \frac{n}{2}$,

$$p_j = \binom{n}{j + \frac{n}{2}} - \binom{n}{j + \frac{n}{2} + 1} = \binom{n + 1}{j + \frac{n}{2} + 1} \frac{q_j}{n + 1},$$

where

$$q_j = 2j + 1 \quad \text{for} \quad j \in \mathcal{J}_n.$$
In the proof below we shall explicitly identify the spatial decomposition that yields this decomposition of $A'_n$. Recall that this is necessary for using the noiseless subsystem approach to quantum error correction. Before proving this theorem, let us illustrate how $\Delta_n$ gives a visual method for determining the commutant structure. For the sake of brevity, let us focus on a single case, the $n = 4$ collective rotation channel $E_4$.

**Example C.6.1.** In the $n = 4$ case we have $J_4 = \{0, 1, 2\}$ and $p_0 = 2, p_1 = 3, p_2 = 1$ and $q_0 = 1, q_1 = 3, q_2 = 5$. The theorem states that

$$\text{Fix}(E_4) = A'_4 = A'_0 \oplus A'_1 \oplus A'_2,$$

with each $A^{(j)}$ a subalgebra of $A'_4$ unitarily equivalent to

$$A'_0 \approx \mathbb{C} \otimes \mathbb{I}_5 \approx \mathbb{C} \mathbb{I}_5,$$

$$A'_1 \approx \mathcal{M}_3 \otimes \mathbb{I}_3,$$

$$A'_2 \approx \mathcal{M}_2 \otimes \mathbb{I}_1 \approx \mathcal{M}_2.$$

Consider the structure of $\Delta_4$ as in Figure C.10. The number $p_j$ corresponds to the ‘height’ of the $j$th horizontal bar (counting top-down), and $q_j$ equals the number of
blocks inside this bar. Spatially, the vertical bars correspond to the eigenspaces for $J_z$ for the eigenvalues $m = -2, -1, 0, 1, 2$ (with eigenspace projections $Q_m$ in the proof below), which have respective multiplicities 1, 4, 6, 4, 1. The horizontal bars correspond to eigenspaces of $J^2$ (Corollary 4.10). The corresponding eigenspace projections $P_0, P_1, P_2$ are the minimal central projections for $A_4$ and $A'_4$.

To see how the blocks correspond to subspaces, the subspace $H_a$, as an example, for the top box in $\Delta_4$ is the joint eigenspace for $J_z$ and $J^2$, corresponding to $m = 0$ and $j = 0$ with our notation below. Each of the $j$th horizontal bars further breaks up into smaller horizontal bars, for instance $P_1 = \sum_{k=1}^{3} P_{1,k}$. The subspaces $\{P_{j,k}\}$ form the maximal family of minimal reducing subspaces for $A_4$ as outlined below. On the other hand, the corresponding family for $A'_4$ is given by the vertical blocks inside the $j$th horizontal bar. For example, the projection onto $H_b$ and the projections onto its other four counterparts in the $j = 2$ bar (which are all 1-dimensional because they lie in the $j = 2$ bar) are the family of minimal $A'_4$-reducing subspaces supported on $P_2$.

We now turn to the proof of Theorem C.6.1. Let $n \geq 1$ be a fixed positive integer. We shall find the structure of $A'_n$ by first computing the structure of $A_n$. We begin by showing how the numeric distribution of the eigenvalues for $J_z$ is linked with $\Delta_n$. In what follows, we use the abbreviated Dirac notation to denote the standard orthonormal basis for $H \equiv H_{2^n} = \mathbb{C}^{2^n}$ with $|\frac{-1}{2}\rangle, |\frac{1}{2}\rangle$ corresponding to the base states of the two-level quantum system ($d = 2$ with our notation in the next section);

$$\left\{ |\vec{i}\rangle = |i_1i_2 \cdots i_n\rangle : i_j \in \{-\frac{1}{2}, \frac{1}{2}\}, 1 \leq j \leq n \right\}. $$

**Lemma C.6.1.** For $m = -\frac{n}{2}, -\frac{n}{2} + 1, \ldots, \frac{n}{2}$ consider the subspaces of $\mathcal{H}$ given by

$$\mathcal{V}_m = \text{span}\left\{|\vec{i}\rangle : |\vec{i}\rangle = m\right\},$$

where $|\vec{i}\rangle = \sum_{j=1}^{n} i_j$. Then $\mathcal{H} = \bigoplus_{m=-\frac{n}{2}}^{\frac{n}{2}} \mathcal{V}_m$ and

$$\dim \mathcal{V}_m = \binom{n}{m + \frac{n}{2}} \quad \text{for} \quad -\frac{n}{2} \leq m \leq \frac{n}{2}.$$ 

Further, $\mathcal{V}_m$ is an eigenspace for $J_z$ corresponding to the eigenvalue

$$\lambda = m \quad \text{for} \quad -\frac{n}{2} \leq m \leq \frac{n}{2}.$$
Proof. The spatial decomposition of $\mathcal{H}$ is easy to see and the dimensions of the $V_m$ follow from simple combinatorics. For the eigenvalue connection with $J_z$, observe that for $|\vec{i}| = m$ we have

$$J_z|\vec{i}\rangle = \sum_{k=1}^{n} J_z^{(k)}|\vec{i}\rangle = \sum_{k=1}^{n} i_k|\vec{i}\rangle = |\vec{i}\rangle = m|\vec{i}\rangle.$$  

For $-\frac{n}{2} \leq m \leq \frac{n}{2}$, let $Q_m$ be the orthogonal projection of $\mathcal{H}$ onto $V_m \equiv Q_m \mathcal{H}$.

Lemma C.6.2. Given $-\frac{n}{2} \leq m \leq \frac{n}{2}$, we have

$$J_+ Q_m = \begin{cases} Q_{m+1} J_+ Q_m & \text{if } m < \frac{n}{2} \\ 0 & \text{if } m = \frac{n}{2} \end{cases}$$

and

$$J_- Q_m = \begin{cases} Q_{m-1} J_- Q_m & \text{if } m > -\frac{n}{2} \\ 0 & \text{if } m = -\frac{n}{2} \end{cases}$$

Proof. Let $|\psi\rangle$ belong to $Q_m \mathcal{H}$. Then $J_z|\psi\rangle = m|\psi\rangle$. But notice that

$$J_z J_+ = J_z (J_x + iJ_y) = J_x J_z + iJ_y J_z + J_z = J_+ (J_z + 1).$$

Thus $J_z J_+|\psi\rangle = (m + 1)J_+|\psi\rangle$ when $m < \frac{n}{2}$, so that $J_+|\psi\rangle$ belongs to $Q_{m+1} \mathcal{H}$. The corresponding identities for $J_-$ are proved in a similar fashion and for convenience the identities $J_+ Q_m = 0 = J_- Q_m$, $m = \frac{n}{2}$, will be observed in the discussion which follows.

Next we shall derive a spatial decomposition of $\mathcal{H}$ which will allow us to connect with the structure of $\Delta_n$. Let

$$|0_L\rangle \equiv |\frac{n}{2}, -\frac{n}{2}, 1\rangle$$

be a (unit) eigenvector for $J_z$ for the eigenvalue $m = -\frac{n}{2}$. The span of $|0_L\rangle$ will be identified with the ‘bottom left corner’ of $\Delta_n$, see Corollary C.6.1 below. To simplify notation, let $ns = \frac{n}{2}$ (the use of this notation will become clear in the next section). Lemma C.6.2 shows that $J_+|0_L\rangle \equiv |ns, -ns + 1, 1\rangle$ is an eigenvector of $J_z$ for the eigenvalue $m = -ns + 1$. Similarly, the vectors

$$J_+^p|0_L\rangle \equiv |ns, -ns + p, 1\rangle \quad \text{for} \quad 0 \leq p < q_{ns},$$
are non-zero and belong to \( V_{-ns+p} \).

Let \( \{|ns-1,-ns+1,\mu\}\}_\mu \) be an orthonormal basis for
\[
V_{-ns+1} \oplus \text{span}\{|ns,-ns+1,1\}.
\]

At this stage the choice of this basis, indexed by \( \mu \), is arbitrary. Now inductively, if we are given \( j \in J_n \) with \( j < ns \), let \( \{|j,m=-j,\mu\}\}_\mu \) be an (arbitrary) orthonormal basis for
\[
V_{-j} \oplus \text{span}\{|j',-j,\mu\} : j < j' \leq ns \},
\]
where \( |j',-j,\mu\rangle = J_j' |j,-j,\mu\rangle \).

Notice that
\[
J_- |j,m=-j,\mu\rangle = 0 \quad \text{for all} \quad j,\mu.
\]
Indeed, by choice of the vectors \( |j,-j,\mu\rangle \) and from the ‘eigenspace shifting’ of Lemma C.6.2, it follows that each \( |j,-j,\mu\rangle \) is orthogonal to the range space of \( J_+ \). Thus \( J_- \) annihilates the left hand steps of \( \Delta_n \), which is the content of (C.61). From this we also have
\[
J_+ |j,m=j,\mu\rangle = J_j^n |j,m=-j,\mu\rangle = 0 \quad \text{for all} \quad \mu.
\]
In other words, from the \( \Delta_n \) picture given by Corollary C.6.1 below, \( J_+ \) annihilates the right hand side blocks of \( \Delta_n \).

Thus, in summary we have a collection of vectors \( |j,m,\mu\rangle \) (which turn out to form an orthogonal basis for \( \mathcal{H} \)) such that: \( j \) belongs to \( J_n \), for fixed \( j \) the range of \( m \) is \( -j \leq m \leq j \), for each \( j,m,\mu \),
\[
|j,m,\mu\rangle = J_j^{(m+j)}|j,-j,\mu\rangle = J_j^{(m-j)}|j,j,\mu\rangle,
\]
and for a given \( m,j \) pair the index \( \mu \) has \( p_j \) possible values.

For fixed \( j,\mu \) let \( \mathcal{H}(j,\mu) \) be the subspace defined by
\[
\mathcal{H}(j,\mu) = \text{span}\{ |j,m,\mu\rangle : -j \leq m \leq j \}.
\]
Such a subspace corresponds to a horizontal slice of the ‘\( j \)th horizontal bar’ in \( \Delta_n \). From Corollary C.6.1, it follows that these subspaces are pairwise orthogonal for distinct pairs \( j,\mu \). (This justifies the use of the orthogonal sum symbol \( \oplus \) in the following statement.)
Lemma C.6.3. The operator $J^2$ belongs to the centre of $A$; that is,

$$J^2 \in A_n \cap A_n'.$$

Consider the subspaces

$$W_j = \sum_{\mu} \oplus \mathcal{H}(j, \mu) \quad \text{for} \quad j \in \mathcal{J}_n.$$

Then the restriction of $J^2$ to each of these subspaces is a constant operator; i.e., there are scalars $\lambda_j$ such that

$$J^2|_{W_j} = \lambda_j 1_{W_j} \quad \text{for} \quad j \in \mathcal{J}_n.$$

Further, these scalars satisfy $\lambda_{j_1} \neq \lambda_{j_2}$ for $j_1 \neq j_2$.

**Proof.** By definition $J^2$ belongs to $A$. We show that $J^2$ commutes with $J_x$. The $J_y$ and $J_z$ cases are similar. Observe that

$$[J_x, J^2] = [J_x, J_y^2 + J_z^2] = [J_x, J_y^2] + [J_x, J_z^2] = J_y [J_x, J_y] + [J_x, J_y] J_y + J_z [J_x, J_z] + [J_x, J_z] J_z = J_y (i J_z) + (i J_z) J_y + J_z (-i J_y) + (-i J_y) J_z = 0.$$

Consider a vector $|j, -j, \mu\rangle$ in the left most block of $W_j$. Observe that $J^2 = J_+ J_- + J_z^2 - J_z$, and hence

$$J^2|_{W_j} = (J_z^2 - J_z)|j, -j, \mu\rangle = (j^2 + j)|j, -j, \mu\rangle.$$

As $J^2$ belongs to $A_n'$, we have $J^2 J_+ = J_+ J^2$. Thus, given a typical basis vector $J_+^{(m+j)}|j, -j, \mu\rangle = |j, m, \mu\rangle$ inside $W_j$ compute

$$J^2(J_+^{(m+j)}|j, -j, \mu\rangle) = J_+^{(m+j)} J^2|j, -j, \mu\rangle = (j^2 + j) J_+^{(m+j)}|j, -j, \mu\rangle = (j^2 + j)|j, m, \mu\rangle.$$

It follows that the corresponding restrictions of $J^2$ satisfy $J^2|_{W_j} = (j^2 + j) 1_{W_j}$, and the scalars $\lambda_j = j^2 + j$ are different for distinct values of $j$.

**Corollary C.6.1.** The vectors $\{|j, m, \mu\rangle\}_{j,m,\mu}$ are non-zero and form an orthogonal basis for $\mathcal{H}$. Thus,

$$\mathcal{H} = \sum_j \oplus W_j = \sum_{j,\mu} \oplus \mathcal{H}(j, \mu),$$

and the subspaces $\{W_j\}$ are the eigenspaces for $J^2$. 
Proof. These vectors are clearly all non-zero by the above discussions. Consider two vectors from this set, $J_+^{p_1}|j_i, m_i, \mu_i\rangle$ for $i = 1, 2$. Then

$$\langle j_1, m_1, k_1|J_+^{p_2-p_1}|j_2, m_2, k_2\rangle = 0 \quad \text{if} \quad (j_1, m_1, k_1) \neq (j_2, m_2, k_2).$$

This follows from the choice of the vectors $|j, m, \mu\rangle$, the relations

$$J_+J_- = J_2^x + J_2^y - J_2^z = J_2^z - J_2^2 - J_z, \quad (C.63)$$

$$J_-J_+ = J_2^x + J_2^y + J_z = J_2^z - J_2^2 + J_z, \quad (C.64)$$

and the connections with the eigenspaces for $J_z, J^2$ given by Lemma C.6.1 and Lemma C.6.3.

The following perspective on the actions of $J_+$ and $J_-$ will be useful below.

**Lemma C.6.4.** For all $j, \mu$, the operators $J_+$ and $J_- = J_+^\dagger$ act as weighted shifts on the standard basis for $\mathcal{H}(j, \mu)$.

Proof. Recall that $J_-|j, m = -j, \mu\rangle = 0$ since $|j, -j, \mu\rangle$ belongs to the orthocomplement of the range of $J_\dagger = J_+$; that is, $\langle j, -j, \mu||J_+\psi\rangle = 0$ for all $|\psi\rangle \in \mathcal{H}$. Thus, by equation (C.64) and Lemma C.6.1 and Lemma C.6.3, for $p \geq 1$ there is a scalar $c$ with

$$J_-J_+^{(m+j)}|j, m, \mu\rangle = (J_2^z - J_2^2 - J_z)J_+^{(m+j-1)}|j, m, \mu\rangle = cJ_+^{p-1}|j, m - 1, \mu\rangle.$$

In particular, $J_-$ acts as a backward shift on the (orthogonal) basis $\{|j, m, \mu\rangle : -j \leq m \leq j\}$ for $\mathcal{H}(j, \mu)$ with $J_-|j, -j, \mu\rangle = 0$. Similarly, by using (C.63) it can be seen that $J_+$ acts as the forward shift on this basis with $J_+|j, j, \mu\rangle = 0$.

Hence, when the basis $\{|j, m, \mu\rangle : -j \leq m \leq j\}$ is normalized to turn it into an orthonormal basis for $\mathcal{H}(j, \mu)$, we see that $J_+$ (respectively $J_-$) acts as a forward (respectively backward) weighted shift on this basis.

The following result shows that the family of mutually orthogonal subspaces $\mathcal{H}(j, \mu)$ forms the (unique) maximal family of minimal reducing subspaces for $A_n$ which determine the minimal central projections.

**Lemma C.6.5.** For all $j, \mu$, the subspace $\mathcal{H}(j, \mu)$ is a minimal $A_n$-reducing subspace.
Proof. First note that $\mathcal{H}(j, \mu)$ is clearly reducing for $J_z$ (i.e. invariant for both $J_+$ and $J_-$). Also, Lemma C.6.4 shows that $\mathcal{H}(j, \mu)$ reduces $J_+$ and $J_-$. Hence $\mathcal{H}(j, \mu)$ is a reducing subspace for $\mathcal{A}_n = \text{Alg}\{J_+, J_-, J_z\}$.

To see minimality, fix $j, \mu$ and let $|\psi\rangle$ be a non-zero vector inside $\mathcal{H}(j, \mu)$. Then by Lemma C.6.4 there is a $p \geq 0$ such that $J_p^\mu |\psi\rangle$ is a non-zero multiple of $|j, -j, \mu\rangle$. Hence, each basis vector $|j, m, \mu\rangle$, for $-j \leq m \leq j$, belongs to the subspace $\mathcal{A}_n |\psi\rangle = \mathcal{H}(j, \mu)$, and it follows that $\mathcal{H}(j, \mu)$ is minimal $\mathcal{A}_n$-reducing.

The structure of $\Delta_n$ determines which of the $\mathcal{H}(j, \mu)$ sum to give the family of minimal central projections. Recall that the minimal central projections of $\mathcal{A}_n$ and $\mathcal{A}'_n$ are the same since $\mathcal{A}_n \cap \mathcal{A}'_n = (\mathcal{A}'_n)' \cap \mathcal{A}'_n$.

Lemma C.6.6. For each $j, \mu$ let $P_{j,\mu}$ be the projection of $\mathcal{H}$ onto $\mathcal{H}(j, \mu) = P_{j,\mu} \mathcal{H}$. Then the minimal central projections for $\mathcal{A}_n$ and $\mathcal{A}'_n$ are $\{P_j\}$ where

$$P_j = \sum_\mu P_{j,\mu},$$

and hence $W_j = P_j \mathcal{H} = \sum_\mu \oplus P_{j,\mu} \mathcal{H}$.

Proof. The projections $P_{j,\mu}$ form the (unique) maximal family of non-zero minimal reducing projections for $\mathcal{A}_n$. Thus, the minimal central projections for $\mathcal{A}_n$ are given by sums of the $P_{j,\mu}$, and so we must find which subsets of the $P_{j,\mu}$ are linked inside $\mathcal{A}_n$ (see (C.56)). Since linked projections amongst the $P_{j,\mu}$ necessarily have the same rank, it is enough to fix $j$ and consider the family $\{P_{j,\mu}\}_\mu$.

In fact, we claim that the entire family $\{P_{j,\mu}\}_\mu$ is linked inside $\mathcal{A}_n$. To see this, it is sufficient, and best for use in the noiseless subsystem method, to exhibit bases for $P_{j,\mu} \mathcal{H}$ which allow us to view the links explicitly. By construction, the basis $\{|j, m, \mu\rangle : -j \leq m \leq j\}_\mu$ for $P_{j,\mu} \mathcal{H}$ used in the analysis above is such a basis. Indeed, we may compute that

$$\langle j, m_1, \mu_1 | J_{p_1}^\mu A J_{p_2}^\mu |j, m_1, \mu_1\rangle = \langle j, m_2, \mu_2 | J_{p_1}^\mu A J_{p_2}^\mu |j, m_2, \mu_2\rangle,$$

for all possible choices of $\mu_1, \mu_2, p_1, p_2$ and $A \in \mathcal{A}_n$. Recall that $\mathcal{A}_n$ is generated by $J_+, J_-, J_z$ as an algebra. By design, (C.65) is evident for $A$ equal to one of these generators, for any monomial in them, and hence, when extending by linearity, for any element of $\mathcal{A}_n$. It follows that for all $j$, the projection $P_j = \sum_\mu P_{j,\mu}$ is a minimal central projection for $\mathcal{A}_n$ (and $\mathcal{A}'_n$). x
Proof of Theorem C.6.1. By the previous result $A_n$ has a block diagonal decomposition $A_n = \sum_{j \in J_n} \oplus A(j)$, where each $A(j)$ is a subalgebra of $A_n$ which is unitarily equivalent to $A(j) \simeq \mathbb{1}_{p_j} \otimes \mathcal{M}_{q_j}$, since $\text{rank } P_{j,\mu} = q_j = \dim \mathcal{H}_{j,\mu}$ for all $\mu$ and there are $p_j$ linked projections $\{ P_{j,\mu} \}_\mu$. Therefore, the commutant $\text{Fix}(E_n) = A_n'$ may be obtained by

$$\text{Fix}(E_n) = A_n' = \sum_{j \in J_n} \oplus A'(j),$$

with $A'(j) \simeq \mathcal{M}_{p_j} \otimes \mathbb{1}_{q_j}$ for $j \in J_n$, as claimed in the statement of Theorem C.6.1. Observe that we also have the minimal reducing projections for $A_n'$ which are supported on the minimal central projections $P_j$. For each $j \in J_n$ they are the projections of rank $p_j$ onto $\text{span}\{ |j, m, \mu \rangle \}_\mu$. Thus, the explicit spatial decomposition of $\text{Fix}(E_n) = A_n'$ is now evident.

The following is a consequence of the work in this section.

**Corollary C.6.2.** The set of spectral projections for $J^2$ coincides with the set of minimal central projections for $A_n'$ and $A_n$.

**Generalized Collective Rotation Channels**

In this section we consider natural generalizations of collective rotation channels to higher dimensional representations of $su(2)$ (see Note C.6.1). The commutation relations satisfied by the Pauli matrices are the defining properties of the Lie algebra $su(2)$. So far, we have restricted our attention to the special case where this algebra is represented by $2 \times 2$ complex matrices; specifically the Pauli matrices. Nevertheless, the algebra $su(2)$ has an irreducible representation for every integer dimension; i.e., given $d \geq 1$ it is possible to find three matrices $\Sigma_{x,d}$, $\Sigma_{y,d}$, $\Sigma_{z,d}$ of dimension $d$ satisfying the Pauli commutation relations. Hence, the rotation group $SU(2)$ also has a representation in every integer dimension.

Note that the operators $J_x, J_y, J_z$, which act on $2^n$-dimensional space, form a representation of the Lie group $su(2)$. But it is not an irreducible representation as the theorem in the last section shows; thus the existence of noiseless subsystems. The irreducible representations of $su(2)$ are determined by restricting these operators to a minimal reducing subspace $\mathcal{H}(j, \mu)$. Indeed, it is easily seen that these are $q_j$-dimensional irreducible representations of the Lie algebra $su(2)$. (The restrictions of $J_x, J_y, J_z$ to each of these irreducible subspaces satisfies the Pauli commutation relations.)
Physicists call a $d$-dimensional representation of $su(2)$ a ‘spin-$s$’ representation, where $d = 2s + 1$. Hence, the spin $s = \frac{d-1}{2}$ can take integer and half integer values. From this more general perspective, we see that in the previous section we considered the spin-$\frac{1}{2}$ ($d = 2$) representation of the rotation group acting on the 2-dimensional Hilbert space of a qubit. Consideration of the proof in the previous section shows that it primarily depends on the commutation relations satisfied by the generators of $su(2)$, not the particular representations of eigenvectors used in the proof. This ‘coordinate-free’ approach allows us to readily generalize our results to collective rotation channels of arbitrary integer dimension. Most of the results from the previous section follow with small modifications, thus we shall only outline the approach.

First let us establish some notation. Let $\Sigma_{k,d}$, $k = x, y, z$, be $(2s+1) \times (2s+1)$ complex matrices forming an irreducible representation of $su(2)$. These matrices act on the $d$-dimensional Hilbert space $H_d$ of a ‘qudit’, where $d = 2s + 1$. Consider a collection of $n$ qudits, and their associated collective rotation generators $J_{x,d}$, $J_{y,d}$, $J_{z,d}$. Let $\mathcal{E}_{n,d}(T) = E_{x,d}TE_{x,d}^\dagger + E_{y,d}TE_{y,d}^\dagger + E_{z,d}TE_{z,d}^\dagger$ where $E_{x,d} = \exp(i\theta_x J_{x,d})$, etc. Let

$$\mathcal{A}_{n,d} = \text{Alg}\{E_{x,d}, E_{y,d}, E_{z,d}\} = \text{Alg}\{J_{x,d}, J_{y,d}, J_{z,d}\},$$

the interaction algebra for the channel. Thus the noise commutant and fixed point set coincide; $\text{Fix}(\mathcal{E}_{n,d}) = \mathcal{A}_{n,d}'$.

**Proposition C.6.3.** The eigenvalues of $\Sigma_{z,d}$ are $-s, -s + 1, \ldots s$, where $s = \frac{d-1}{2}$.

**Proof.** This follows from the definition of $\Sigma_{z,d}$ as the restriction of the operator $J_z$ on $\mathcal{H}(s, \mu)$. As in the qubit case ($s = \frac{1}{2}$, $d = 2$), we can thus represent a vector in $\mathcal{H}_d^n$ by $|\vec{i}\rangle = |i_1 i_2, \ldots i_n\rangle$ where $i_k \in \{-s, -s+1, \ldots s\}$ denotes the eigenvalue of $\Sigma_{z,d}$ on the $k$th qudit. With this notation, we can restate Lemma C.6.1 for arbitrary finite dimension $d$.

**Lemma C.6.7.** For $m = -sn, sn + 1, \ldots, sn$ consider the subspaces of $\mathcal{H}_d^n$ given by

$$\mathcal{V}_m = \text{span}\{ |\vec{i}\rangle : |\vec{i}\rangle = m\}.$$
where \(|\vec{i}\rangle = \sum_{j=1}^{n} i_j\). Then \(\mathcal{H}_{d^n} = \sum_{-sn \leq m \leq sn} \oplus \mathcal{V}_m\) and

\[
\dim \mathcal{V}_m = \sum_{k_1 + \ldots + k_n = m + ns} \binom{n}{k_1 \ldots k_n},
\]

where \(k_i \in \{0, \ldots, d - 1\}\) and no repeats are allowed, even reordering, amongst the \(n\)-tuples \((k_1, \ldots, k_n)\). Further, \(\mathcal{V}_m\) is an eigenspace for \(J_z\) corresponding to the eigenvalue \(m\).

The proof of this Lemma follows exactly the same lines as Lemma C.6.1. The analogues of Lemmas C.6.2 and C.6.3 also follow in a straightforward manner; they only involve the commutation relations which are independent of the representation of the algebra.

We can thus construct a basis for \(\mathcal{H}_{d^n}\) by generalizing the previous construction. The basis states are \(|j, m, \mu\rangle\). The label \(j\) is for the eigenspaces of the operator \((J^{(d)})^2 \equiv J_{x,d}^2 + J_{y,d}^2 + J_{z,d}^2\) which has eigenvalues given by \(j^2 + j\) with \(j \in \mathcal{J}_{n,d}\) where

\[
\mathcal{J}_{n,d} = \begin{cases} 
\{0, 1, \ldots, ns\} & \text{if } ns \text{ is an integer} \\
\{\frac{1}{2}, \frac{3}{2}, \ldots, ns\} & \text{if } ns \text{ is a half integer}
\end{cases}
\]

The eigenspaces of \(J_{z,d}\) are labelled by \(m\), where \(m = -j, -j + 1, \ldots, j\) (Recall that \((J^{(d)})^2\) and \(J_{z,d}\) commute, so they can be simultaneously diagonalized.) Finally, \(\mu\) is the extra index required to construct a basis in the common eigenspace of \((J^{(d)})^2\) and \(J_{z,d}\) determined by a given pair \(j, m\).

Let us construct these states as we did in the previous section. We start with the state \(|ns, -ns, 1\rangle\) which is the unique eigenvector of \(J_{z,d}\) with eigenvalue \(-ns\). It is thus an eigenvector of \((J^{(d)})^2\). Then, \(J_{+,d} |ns, -ns, 1\rangle\) is an eigenstate of \(J_{z,d}\) with eigenvalue \(-ns + 1\). Furthermore, since \(J_{+,d}\) commutes with \((J^{(d)})^2\), the vectors \(J_{+,d} |ns, -ns, 1\rangle\) and \(|ns, -ns, 1\rangle\) are in the same eigenspace of \((J^{(d)})^2\); hence after normalizing we can label \(J_{+,d} |ns, -ns, 1\rangle\) by \(|ns, -ns + 1, 1\rangle\). By repeating this procedure, we find an orthonormal basis for the space

\[
\mathcal{H}(ns, 1) = \text{span}\{ (J^{(d)}_+)^p |ns, -ns, 1\rangle : 0 \leq p \leq 2ns \}
\]

\[
= \text{span}\{ |ns, m, 1\rangle : m = -ns, -ns + 1, \ldots, ns \}.
\]

By construction, \(\mathcal{H}(ns, 1)\) is a minimal reducing subspace for \(A_{n,d}\). Furthermore, since the spectral projections of \((J^{(d)})^2\) are the minimal central projectors of \(A_{n,d}\), the subspace \(\mathcal{H}(ns, 1)\) is an eigenspace of \((J^{(d)})^2\).
We then consider the subspace $\mathcal{V}_{-ns+1} \ominus \text{span}\{|ns, -ns+1, 1\}$. This is the eigenspace of $J_{z,d}$ with eigenvalue $m = -ns + 1$ which is perpendicular to the eigenspace of $(J^{(d)})^2$ labelled by $ns$. Hence, these vectors require a different $j$ label, say $j = ns - 1$. We can now choose a basis for $\mathcal{V}_{-ns+1} \ominus \text{span}\{|ns, -ns+1, 1\}$, which is labeled $|ns-1, -ns+1, \mu\rangle$ where the first two terms just label the subspace $\mathcal{V}_{-ns+1} \ominus \text{span}\{|ns, -ns+1, 1\}$ and $\mu$ is an extra label to form a basis within this subspace. Thus, as we did in the previous section, we construct subspaces by applying the shift operator

$$
\mathcal{H}(ns-1, \mu) = \text{span}\{J_{+,d}^p|ns-1, -ns+1, \mu\rangle : 0 \leq p \leq 2(ns-1)\} \\
= \text{span}\{|ns-1, m, \mu\rangle : -ns+1 \leq m \leq ns-1\}.
$$

This procedure can be repeated with the subspaces

$$
\mathcal{V}_{-m} \ominus \text{span}\{|j, -m, \mu\rangle : j = m + 1, \ldots ns, \mu = 1, \ldots, q_j\}
$$

to form the subspaces

$$
\mathcal{H}(j, \mu) = \text{span}\{J_{+,d}^p|j, -j, \mu\rangle : 0 \leq p \leq 2j\} \\
= \text{span}\{|j, m, \mu\rangle : -j \leq m \leq j\}.
$$

The subspaces $\mathcal{H}(j, \mu)$ are minimal $\mathcal{A}_{n,d}$-reducing and for fixed $j$, the subspaces $\{\mathcal{H}(j, \mu)\}_\mu$ are linked inside $\mathcal{A}_{n,d}$. Thus with this analysis in hand, we may state the following generalization of Theorem C.6.1.

**Theorem C.6.2.** Let $\mathcal{E}_{n,d}$ be the collective rotation channel for fixed positive integers $n \geq 1$ and $d \geq 2$. Then

$$
\text{Fix}(\mathcal{E}_{n,d}) = \mathcal{A}'_{n,d} = \sum_{j \in \mathcal{J}_{n,d}} \oplus \mathcal{A}'_{(j)},
$$

where $\mathcal{A}'_{(j)}$ is a $C^*$-subalgebra of $\mathcal{A}'_{n,d}$ given, up to unitary equivalence, by

$$
\mathcal{A}'_{(j)} \simeq \mathcal{M}_{p_j} \otimes \mathbb{1}_{q_j} \quad \text{for} \quad j \in \mathcal{J}_{n,d},
$$

with $p_{ns} = 1$ where and for $j \in \mathcal{J}_{n,d}$, $j < ns$,

$$
p_j = \dim \mathcal{V}_j - \dim \mathcal{V}_{j+1}
$$

where

$$
q_j = 2j + 1 \quad \text{for} \quad j \in \mathcal{J}_{n,d}.
$$
Remark C.6.1. In light of this analysis, we can extend the result to more general Lie groups. Let \( G \) be a compact connected semisimple Lie group and \( G^{\otimes n} \) denote its \( n \)-fold tensor product. Further, let \( \Sigma_k \) be the set of generators of the associated Lie algebra. This algebra is entirely specified by its structure constants \( C_{kmn} \) defined by
\[
[\Sigma_m, \Sigma_n] = i \sum_k C_{kmn} \Sigma_k. \tag{C.67}
\]

The operators
\[
J_k = (\Sigma_k \otimes \mathbb{I} \otimes \mathbb{I} \otimes \ldots) + (\mathbb{I} \otimes \Sigma_k \otimes \mathbb{I} \otimes \ldots) + \ldots \tag{C.68}
\]
are generators of the generalized ‘collective rotation’ which is a subgroup of \( G^{\otimes n} \). Clearly, they have the same structure constants has the \( \Sigma_k \); they represent the same algebra. Nevertheless, the \( J_k \) do not form an irreducible representation of the algebra. Hence, it is possible to write them as a direct sum of irreducible representations. A special property of these representations is that all the projections onto the irreducible subspaces of the same dimension are in fact ‘linked’ inside the algebra. Thus, it follows that there is an abundance of noiseless subsystems which can be explicitly identified for the corresponding quantum channels. An expansion of this analysis is contained in [JKK04a].

Acknowledgements. We would like to thank Marius Junge and Peter Kim for helpful conversations. We are grateful for support from the Perimeter Institute, the Institute for Quantum Computing, the University of Guelph, NSERC, MITACS, and ARDA.
Bibliography


BIBLIOGRAPHY


[Cav00a] Caves, C. Betting probabilities and the Dutch book, 2000. At this URL.


BIBLIOGRAPHY


