On Experimental Deterministic Quantum Computation with One Quantum Bit (DQC1)

by

Gina Passante

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

Waterloo, Ontario, Canada, 2012

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

G. Passante

Abstract

Quantum information processors have the ability to drastically change our world. By manipulating bits of information ruled by the laws of quantum mechanics, computational devices can perform some computations that are classically intractable. Most quantum algorithms rely on pure qubits as inputs and require entanglement throughout the computation. In this thesis, we explore a model of computation that uses mixed qubits without entanglement known as DQC1 (deterministic quantum computation with one quantum bit), using the physical system of liquid-state Nuclear Magnetic Resonance (NMR). Throughout our research, we experimentally implement an algorithm that completely encapsulates the DQC1 model, and take a close look at the quantum nature of DQC1-states as given by the quantum discord and geometric quantum discord, which are measures of non-classicality that capture correlations weaker than those measured by entanglement. We experimentally detect and quantify these correlations in an NMR DQC1 quantum information processor.

Acknowledgements

First and foremost, I would like to thank my supervisor Prof. Raymond Laflamme, who provided me with guidance, allowed me the freedom to study the questions that were most interesting to me, and always came up with timely and thought-provoking ideas and questions. My advisory committee of, Prof. Joseph Emerson, Prof. Kevin Resch, and Prof. Jonathan Baugh, were extremely helpful by providing insights and asking the right questions in my committee meetings. I would also like to thank Prof. Dieter Suter for agreeing to sit on the examining committee. Dr. Colm Ryan was ever so patient when teaching me how to use the spectrometer, and took the time to help me understand the matlab codes he had written. Mike Ditty, I am sorry for all the emails indicating that I 'broke the spectrometer'. (For the record, no spectrometers were harmed in the making of this thesis.) In all seriousness, Mike provided me with assistance and technical support, without which my experiments would not have been possible. Dr. Osama Moussa has been a most excellent collaborator and friend. Every project in this thesis has benefitted greatly from his involvement, for which I am truly indebted.

Waterloo has become my home because of the amazing friends I have made. I won't attempt to name all of them, but want to acknowledge Chris for being a wonderful thesis writing companion, whose timely emails of encouragement offered the push I needed to continue writing. Osama, who never fails to offer perspective and advice, and is always there to lend a hand, ear or shoulder. Also, without the #uptownknitmob this journey would not have been the same. You are truly the best group of friends I have ever met and I feel honoured to be a part of your lives. I specifically need to thank you for listening to my thesis-writing tweets, never failing to offer food or companionship, and helping to edit my thesis.

Last, but certainly not least, I have to thank my family. They have been a constant source of love, support, and encouragement. My mom has sacrificed so much in order for me to have the life I did. She always believes in me and taught me that I can accomplish anything I put my mind to. Selina is the most wonderful sister and friend - thank you for always being there for me. You don't realize just how inspiring you are.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Devices for processing quantum information are currently in transition from figments of science fiction to reality in laboratories across the globe. Quantum information and computation promise to drastically change the course of technology and society. Researchers have already achieved important milestones – from teleporting a quantum state [BPM+97, NKL98] to perfectly securing election ballots using quantum cryptography [Gre07] – and the biggest breakthroughs of the quantum revolution are yet to come. However, there is a long road ahead before we have quantum gadgets in our homes and offices. Since the first quantum computers were experimentally realized around the turn of the 21st century, many different technologies for manipulating quantum bits, or qubits, have been developed in the hopes of becoming the industry standard.

A qubit is the fundamental unit of information in a quantum information processor and is physically realized in a system whose observables are the Pauli matrices. One of the earliest implementations of quantum algorithms was performed in Nuclear Magnetic Resonance (NMR), where the qubits are encoded in the energy eigenstates of spin-1/2 nuclei. NMR quantum computers have been used to implement Deutsch's problem [JM98, CVZ+98, LBF98], Shor's algorithm for factoring numbers [VSB+01], simulating quantum systems [STH+99, TSS+99, NSO+05, CYC06], and magic state distillation [SZRL11], to name a few. Furthermore, NMR allows for incredible control over small quantum systems [RLL09].

One of the drawbacks to NMR quantum computing is the highly mixed states of the qubits when computations are performed at room temperature. Most quantum algorithms

require the initial state preparation be composed of pure states, which are not readily available in the NMR architecture. Another drawback is that there is no entanglement in these systems – a hurdle that, until recently, had been thought to preclude NMR as truly *quantum* computing.

Instead of trying to overcome these drawbacks, the DQC1 model of computation takes an entirely different stance. DQC1 stands for Deterministic Quantum Computation with One Quantum Bit, and is the broad topic of this thesis. The model was introduced in 1998 by E. Knill and R. Laflamme [KL98], and uses a highly mixed initial state to perform a computation that has no known efficient classical algorithm. One of the most interesting features of the DQC1 model is that it contains very little or no bipartite entanglement. To be precise, the DQC1 model contains zero entanglement across the most natural bipartite splitting, and has the potential for a small amount of entanglement across any other bipartite split. The obvious question is what, if not entanglement, is the cause of the apparent advantage in the DQC1 model? In addition, this model calls into question the notion that entanglement is a distinguishing marker of quantum systems.

While entanglement has certainly been the most popular form of quantum correlations discussed, it is not the only one. Recently, the measure of quantum correlations called *quantum discord* [HV01, OZ01] has been at the forefront of research in quantum information theory. This measure was discovered in the early 2000s and is based in the possibility of a local measurement disturbing a distributed quantum state. Mixed states that do not have entanglement, like the ones present in NMR, still have the potential to contain non-classical correlations as measured by the quantum discord. In addition to quantum discord, there have been several other measures of quantum correlations created, as the community tries to determine the defining characteristics of a quantum system.

These questions have driven the research presented in this thesis. We take an experimental look at the DQC1 model of computation and the quantum correlations present in it. The vehicle for our experiments is liquid-state NMR which, due to the prevalence of mixed states, is an ideal system for realizing DQC1. Throughout this thesis we present an implementation of a physically relevant, complete problem for the DQC1 model, as well as test for and measure the quantum correlations present in DQC1 and its NMR implementation. The paragraphs below outline in more detail the composition of this thesis.

Chapter 2 presents the background material required: Section 2.1 explains mixed-state quantum computation, which includes an introduction to both NMR and the DQC1

model of computation, and Section 2.2 provides an introduction to quantum correlations. Specifically, we discuss entanglement and quantum discord, going through several examples to increase our familiarity with these sometimes counterintuitive concepts.

Chapter 3 presents the results of an experiment to approximate the Jones polynomial. This problem has significance in statistical physics, quantum field theory, and applied mathematics [Kau91]; and is of great interest because there is currently no classical algorithm to approximate it efficiently. In 2007, approximating the Jones polynomial at a particular point was shown to completely encapsulate the power of the DQC1 model. We modify the original algorithm and experimentally differentiate six different knots using liquid-state NMR. This experiment is a practical application of mixed-state quantum computation that pushes the boundaries of our current control in NMR.

In Chapter 4, we look for a signature of non-classical correlations, as measured by the quantum discord, in an NMR implementation of a DQC1 algorithm. The amount of quantum discord present in our experimental setup is numerically calculated to be very small (on the order of 10^{-11}), and we set out to determine if this is detectable with our current level of control. To do this we use an experimentally friendly *discord witness* [DVB10].

After detecting quantum correlations in a DQC1 experiment (from Chapter 4), we look to quantify the amount of correlations present. Previously, the only way to do this was to use full knowledge of the quantum state and perform a numerical optimization. This procedure does not scale well as we increase the size of the system, so we set out to find an analytical expression for the amount of quantum correlations in a DQC1-state. We were able to find an expression for the correlations that can be experimentally measured using a DQC1 algorithm. Details and experimental data are found in Chapter 5.

Each research question investigated in this thesis falls under the umbrella of the DQC1 model of mixed-state quantum computation, and was motivated by the desire to better understand what makes a quantum computer *quantum*. We do not claim to have found the answer, but the work presented here plays a crucial role in this quest, as we investigate a very intriguing model of computation and the *quantumness* it contains.

Chapter 2

Background: Mixed-state quantum computation and quantum correlations

In this chapter we will introduce the background material necessary for full appreciation of the material presented in subsequent chapters. It will also serve to establish the terminology, both mathematical and linguistic, that will persist throughout this work. The background material is separated into two sections: Section 2.1, mixed states for quantum information processing and Section 2.2, quantum correlations. Both will give the basic understanding that is required and direct to more resources should your curiosity get the better of you.

2.1 Mixed states for quantum information processing

Mixed-state quantum computation is a common thread that binds this thesis work together. It simply refers to quantum computation with the use of mixed states, which is in contrast to quantum computation with the use of pure initial states. The first step to understanding mixed state computation is having a solid grasp of mixed states: how they are created, evolve, and behave under measurement. This information is given in Section 2.1.1 (a good reference for the material is [NC00]). In Section 2.1.2 we discuss the physical system of

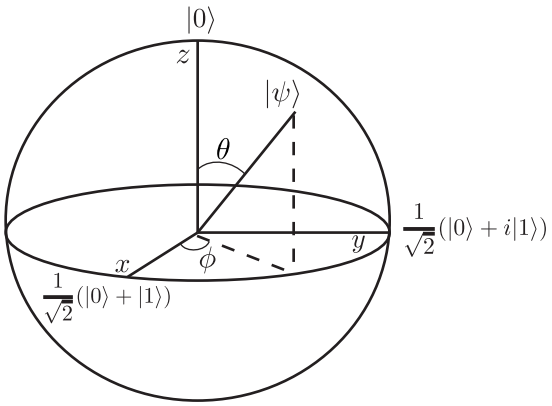

Figure 2.1: The Bloch sphere is a graphical depiction of single qubit states. All pure qubits lie on the surface of the sphere with orthogonal states located at opposite sides. For instance, the two orthogonal states $|0\rangle$ and $|1\rangle$ are located at the top and bottom of the sphere, respectively. Mixed states live in the volume of the sphere, anywhere beneath the surface. The maximally mixed state $\rho = I/2$ is located at the centre.

Nuclear Magnetic Resonance (NMR) that naturally provides us with mixed states for use in our experiments. Finally, in Section 2.1.3 we will discuss a model of computation that utilizes mixed states, known as DQC1, or deterministic quantum computation with one quantum bit, that can solve some problems better than current classical methods.

2.1.1 Mixed states

Most of the protocols in quantum information are described in the context of state vectors $|\psi\rangle$, called *pure states*. A general, single-qubit pure state can be written as

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \tag{2.1}$$

where θ and ϕ have a very nice geometrical representation in what is called the Bloch sphere, pictured in Figure 2.1. Pure states lie on the surface of the Bloch sphere, and orthogonal vectors, somewhat counterintuitively, lie antiparallel to each other. The computational basis states are depicted along the z-axis, with $|0\rangle$ at the top and $|1\rangle$ at the bottom.

However, the set of single qubit states is not limited to the surface of the Bloch sphere, but rather to its volume. The states that lie inside the surface are called *mixed states*.

Both pure and mixed states can be mathematically described by the *density matrix* ρ. Density matrices are operators on the Hilbert space (often referred to as density operators) and are the most general way of describing physical quantum systems. Density matrices are positive operators ($\langle i|\rho|i\rangle$ is real and positive semi-definite for any $|i\rangle$) and have a trace of one ($\mathrm{Tr}(\rho) = 1$). The density operator of a pure state is written as the projection operator

$$\rho_{pure} = |\psi\rangle\langle\psi|.$$

Occasionally, our only description of the physical system is that of a *mixture* where we have state $|\psi_1\rangle$ with probability p_1 and $|\psi_2\rangle$ with probability p_2, and is where the density operator representation becomes necessary. The state of the system in this situation is represented by

$$\rho_{mixture} = p_1|\psi_1\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2|.$$

More generally, the density operator of such a mixture of pure states can be written as

$$\rho_{mixed} = \sum_i p_i|\psi_i\rangle\langle\psi_i|, \tag{2.2}$$

where $\sum_i p_i = 1$. This convex combination of projectors is known as an incoherent mixture, while a linear coherent superposition of the form $|\psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle$ is a pure state.

Any single qubit state can be written in terms of the operators $\{I, X, Y, Z\}$ as

$$\rho_{mixed} = \frac{1}{2}(I + \vec{a}\cdot\vec{\sigma}) = \frac{1}{2}(I + a_x X + a_y Y + a_z Z), \tag{2.3}$$

where I is the identity operator and $\vec{\sigma} = \{X, Y, Z\}$ is the vector of Pauli operators $\{\sigma_x, \sigma_y, \sigma_z\}$. The vector $\vec{a}$ is called the Bloch vector and completely specifies the location of the state ρ on the Bloch sphere – it falls on the surface of the sphere only when $|\vec{a}| = 1$, which is the condition for pure states. Since a density operator can refer to both pure and mixed states it is not always apparent which type of state you have. A quick test for whether a density matrix represents a pure or mixed state is to take the trace of the operator squared; if the state is pure then $\mathrm{Tr}(\rho^2) = 1$ whereas, if the state is mixed, then $\mathrm{Tr}(\rho^2) < 1$. The maximally mixed state of N qubits, $\rho = I/d$ where $d = 2^n$ is the dimension of the n qubits, has $\mathrm{Tr}(\rho^2) = 1/d$. The maximally mixed state of a single qubit lies at the very centre of the Bloch sphere.

Time evolution of a closed system is described by a unitary matrix U, and the evolved state is written as

$$\rho_f = U\rho_i U^\dagger, \tag{2.4}$$

where $U^\dagger$ is the conjugate transpose of U. If a measurement described by the operators $\{M_k\}$ is performed, then the probability of outcome k is defined as

$$p(k) = \mathrm{Tr}(M_k^\dagger M_k \rho), \tag{2.5}$$

and the state after measurement is

$$\rho_k = \frac{M_k \rho M_k^\dagger}{p(k)} = \frac{M_k \rho M_k^\dagger}{\mathrm{tr}(M_k^\dagger M_k \rho)}. \tag{2.6}$$

For a general measurement M, the only restriction on the measurement operators is the completeness relation

$$\sum_i M_i^\dagger M_i = I. \tag{2.7}$$

For projective measurements $\{\Pi_i\}$, in addition to the completeness relation (rewritten as $\sum_i \Pi_i = I$), the following must hold true:

$$\Pi_i \Pi_j = \delta_{ij} \Pi_i. \tag{2.8}$$

When we introduced mixed states at the beginning of this section, we described them as a mixture of pure states, but this is not always practical. For instance, imagine that you have a two qubit state ρ_{AB}, but only want to characterize part of it. Perhaps you gave one of the qubits to your friend and want to describe the state of your remaining qubit. Mathematically, in order to retrieve the state of one subsystem, we use the partial trace operation. The density operator of system A is called the *reduced density operator* and is defined as

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}), \tag{2.9}$$

where the partial trace over system B is defined as

$$\mathrm{Tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| \mathrm{Tr}(|b_1\rangle\langle b_2|), \tag{2.10}$$

and $|a_1\rangle$, $|a_2\rangle$ are any vectors on subsystem A, while $|b_1\rangle$, $|b_2\rangle$ are any vectors on subsystem B.

As a concrete example, let us take one of the pure Bell states $|\psi_{Bell}\rangle = 1/\sqrt{2}(|00\rangle+|11\rangle)$, which is described by the density operator

$$\begin{aligned}\rho_{Bell} &= |\psi_{Bell}\rangle\langle\psi_{Bell}| \\ &= \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{2.11}$$

The reduced density matrix of the first qubit can be found by tracing out qubit B as follows:

$$\rho_A = \mathrm{Tr}_B(|\psi_{Bell}\rangle\langle\psi_{Bell}|) = \sum_i {}_B\langle i|\psi_{Bell}\rangle\langle\psi_{Bell}|i\rangle_B, \tag{2.12}$$

where $\{|i\rangle_B\}$ is any basis on system B, and reduces to

$$\begin{aligned}\rho_A &= {}_B\langle 0|\psi_{Bell}\rangle\langle\psi_{Bell}|0\rangle_B + {}_B\langle 1|\psi_{Bell}\rangle\langle\psi_{Bell}|1\rangle_B \\ &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

This means that a measurement on system A has a 50% probability of resulting in 0 or 1. Examining the reduced density matrix of the second qubit,

$$\rho_B = \mathrm{Tr}_A(\rho_{Bell}) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.13}$$

you find the exact same result. The state ρ_{Bell} is maximally *entangled*, and one of the properties of maximally entangled states is that their reduced density operators are equal to the completely mixed state. Entanglement is a form of quantum correlations, that will be defined and discussed in Section 2.2.1.

Mixed states are very common in nature; a single qubit is very likely coupled to its environment and once the environment is traced out, the state of the qubit is almost always a mixed state. Despite the prevalence of mixed states in the real world, most research for quantum information processing deals with pure qubits. This thesis works within the

realm of mixed state computation, using extremely mixed states (states very close to the completely mixed state) for quantum computational tasks that offer an advantage over current classical methods.

2.1.2 Nuclear Magnetic Resonance for Quantum Information Processing

Nuclear Magnetic Resonance (NMR) quantum information processors utilize the two spin states of spin-1/2 nuclei in a strong magnetic field as their qubit. By finding a molecule with n distinguishable spin-1/2 nuclei, it is possible to construct an n-qubit quantum information processor. The experimental samples used contain many (on the order of 10^{20}) identical molecules and are processed in parallel, resulting in bulk ensemble computation. There are many references that explain the intricacies of NMR for use as a quantum information processor (for example, see [VC04, BCCea07, Jon01]), hence a detailed description will not be provided here. Instead, this section will give a quick overview of the information necessary to understand the remainder of this thesis and lay the ground work for discussing NMR as a mixed-state quantum information processor.

Spin-1/2 particles in the presence of a strong magnetic field are well-behaved qubits: the form of the Hamiltonian of the system is well known, fairly easy to characterize, and the values of T_1 and T_2 on the order of seconds, which allows use of multi-gate algorithms before decoherence effects affect the computation. In addition, NMR benefits from years of development by scientists who used the technology to characterize molecules and proteins, or image the human body. The wealth of knowledge and experience with NMR has allowed quantum information scientists to perform gates with excellent precision [RLL09] and implement some of the very first quantum algorithms [JM98, JMH98, CVZ$^+$98].

As mentioned above, in the presence of a magnetic field, the ground state of a spin-1/2 nucleus undergoes *Zeeman splitting* into two spin levels, which are used to encode each qubit. Let us now look at the individual terms that comprise the Hamiltonian. (For more information, a good introductory level reference for NMR is the book *Spin Dynamics* [Lev08].) The Zeeman Hamiltonian has the form

$$\mathcal{H}_Z = -\sum_i 2\gamma_i \vec{\sigma_i} \cdot \vec{B} = -\sum_i 2\gamma_i B^0 Z_i, \tag{2.14}$$

where γ is the gyromagnetic ratio, $\vec{\sigma}$ is the vector of Pauli matrices, $\vec{B}$ is the external magnetic field and subscript i refers to the i^{th} spin. This convention will be used throughout. It is always assumed that the external magnetic field is in the z-direction, simplifying the Zeeman Hamiltonian. In addition, we represent the Pauli matrices $\{\sigma_x, \sigma_y, \sigma_z\}$ as X, Y, and Z and the identity operator is denoted as I. The dimension of the identity operator is occasionally written explicitly, but can often be inferred from context. Finally, the notation Z_i is understood to mean the Pauli-z operator on the i^{th} spin, while the identity is performed on all others. For example, X_2 on four qubits is the operation $I \otimes X \otimes I^{\otimes 2}$, where $I^{\otimes n}$ is the Kronecker product of I with itself n times.

The Zeeman term of the Hamiltonian is customarily combined with the chemical shift, which is a small change in the Larmor frequency due to the different chemical environments of each nuclei. This is what allows us to distinguish two protons, for instance, in the same molecule (provided there is an absence of symmetry). The single qubit Hamiltonian is then simply written as

$$\mathcal{H} = \pi \omega_i Z_i, \tag{2.15}$$

where ω_i is the chemically shifted Larmor frequency, given in Hertz.

The two main interaction terms of the Hamiltonian are the direct dipole-dipole coupling and the indirect dipole-dipole, or J-coupling. The direct dipole-dipole coupling is the interaction of two spins directly through the space between them. The form of this interaction is proportional to $(3\cos^2\Theta_{jk} - 1)$, where Θ_{jk} is the angle between the static magnetic field and the vector joining spins j and k. In a liquid, the rapid tumbling and translational motion of the molecules averages the dipole-dipole coupling to zero for both intra- and intermolecular interactions. Because all of the experimental work presented in this thesis is performed in the liquid state, dipolar coupling does not play a role.

The J-coupling is a much weaker interaction between two nuclei, as it is mediated through bonding electrons (hence the name *in*direct dipole-dipole). The J-coupling Hamiltonian is

$$\mathcal{H}_J = \sum_{j<k} \frac{\pi}{2} J_{jk} (X_j X_k + Y_j Y_k + Z_j Z_k). \tag{2.16}$$

In the weak coupling limit, where

$$\pi J_{jk} \ll |\omega_j - \omega_k|, \tag{2.17}$$

the secular approximation becomes valid and the Hamiltonian reduces to

$$\mathcal{H}_J = \sum_{j<k} \frac{\pi}{2} J_{jk} Z_j Z_k. \tag{2.18}$$

In the secular approximation, very small terms that do not commute with the large components of the Hamiltonian can be ignored, which, in this case, are the off-diagonal elements. Therefore, in the weak coupling regime of liquid state NMR, the internal Hamiltonian can be written as

$$\mathcal{H}_{int} = \sum_i \omega_i Z_i + \sum_{j<k} \frac{\pi}{2} J_{jk} Z_j Z_k. \tag{2.19}$$

Control of the molecule is achieved by applying radio frequency (r.f.) fields to augment the Hamiltonian of the system in order to perform the desired operation. The control Hamiltonian in the rotating frame of the nuclei is of the form

$$\mathcal{H}_{control} = \omega_{nut}(t)(\cos\phi(t)X + \sin\phi(t)Y), \tag{2.20}$$

where the *nutation frequency* $\omega_{nut}(t)$ and the phase $\phi(t)$ are user-defined. Single qubit rotations are implemented by applying the r.f. fields at the particular resonant frequency of the nuclei to be affected. Multiple qubit gates are easily performed in NMR by utilizing the J-coupling of the internal Hamiltonian. Pulse design has evolved in recent years, enabling experimentalists to 'intelligently' numerically optimize pulses that perform complicated unitary evolutions. This is achieved by discretizing the pulses at small time intervals where the nutation frequency and phase are constant. The propagator at each time step is evaluated and the derivative of the gate fidelity is used to iteratively improve the pulse. The experiments described in this thesis use pulses that are generated by a gradient accent pulse engineering (or GRAPE) algorithm [KRK$^+$05, RNL$^+$08]. The GRAPE algorithm offers a more efficient searching method by using previously estimated parameters to estimate the propagator at each time step, which allows for the use of more searching parameters. For instance, increasing the number of time steps leads to smoother, easier to implement pulses. In addition, it is possible to optimize over a range of r.f. powers to combat inhomogeneities in the r.f. field seen across the sample. Technical information about the codes used to generate the pulses in this thesis were primarily written by Dr. Colm Ryan and details can be found in his doctoral dissertation [Rya08].

One of the drawbacks to using NMR as a fully functional quantum computer is that the thermal state is highly mixed. The thermal state of an n-qubit homonuclear liquid-state

NMR quantum computer is

$$\rho_{th} \approx \frac{1}{2^n} I + \frac{\mathbb{B}}{2^{n+1}} \sum_i Z_i, \tag{2.21}$$

where

$$\mathbb{B} = \frac{\hbar \gamma B^0}{k_B T} \tag{2.22}$$

is the Boltzmann factor and $k_B T$ is the thermal energy. If the different spins in the system are for different nuclear species, then each species will have its own Boltzmann factor. The experiments in this thesis are performed on carbon-13 nuclei ($\gamma = 6.728284 \times 10^7$ rad $\mathrm{T}^{-1} s^{-1}$) at room temperature in a 16.7 T magnet, resulting in a Boltzmann factor of $\mathbb{B} = 2.93 \times 10^{-5}$. The identity portion of the thermal state remains in the identity state throughout the evolution and is not measured during an experiment, so it is often left out of the description and only the *deviation density matrix* is described. The deviation density matrix in Eqn. (2.21) is $\rho_{dev} \propto \sum_i Z_i$, and as you can see, it is not a true density matrix since $\mathrm{tr}(\rho_{dev}) = 0$. To avoid dealing with traceless density matrices, in this thesis NMR states will almost always be written in the form

$$\rho_{NMR} = \frac{(1-\alpha)}{2^n} I + \alpha \rho_{pps}, \tag{2.23}$$

where α is referred to as the polarization and ρ_{pps} is the pseudopure state with unit trace. If we write Eqn. (2.21) in the form of ρ_{NMR}, then the value of the polarization is a fraction of the Boltzmann factor. It is worth noting that ρ_{pps} need not be pure and that the name is used primarily for historical reasons. The polarization for experiments in this thesis is on the order of 10^{-5}. A polarization this small has implications for the entanglement present in the system – but this discussion is left for Section 2.2.

The highly mixed thermal states of a liquid-state NMR experiment make it very difficult to create the initial states, such as $|00\ldots0\rangle$, that are used in pure-state quantum computation. While there exist procedures to create such states in NMR, that is not the approach taken in this work. Instead, the mixed nature of NMR states is utilized to perform algorithms designed for such systems, using mixed-state computational models to solve problems with no known efficient classical analogue.

Measurements in NMR are not the typical projection measurements often used in pure-state quantum computation. Instead, the system is continually measured using a pickup coil, where the magnetic moments of the nuclei induce an electric current in the coil.

This signal is called the free-induction decay (FID) or simply the NMR signal. A Fourier transform of the FID produces an NMR spectrum (an example of an NMR spectrum can be seen in Figure 3.16 from Chapter 3). The coil used to detect the NMR signal is the same coil that implements the r.f. pulses, and is positioned perpendicular to the static magnetic field. This means that it only detects transverse magnetization:

$$M_x(t) = \mathrm{Tr}(\rho(t)\sigma_x) \text{ and} \tag{2.24}$$
$$M_y(t) = \mathrm{Tr}(\rho(t)\sigma_y). \tag{2.25}$$

By observing the frequency of a particular spin for a given time, we are able to determine $\langle\sigma_x\rangle$ and $\langle\sigma_y\rangle$ by integrating the total spectrum. (The signal will be split into several peaks due to the coupling terms in the Hamiltonian.) In order to measure the signal parallel to the static magnetic field, a readout pulse is required. The readout pulse rotates the magnetization in the $x-y$ plane. As we will discuss in Section 4.2, it is possible to apply different readout pulses to measure different operators.

2.1.3 Deterministic Quantum Computation with One Quantum Bit

While most quantum algorithms use pure states as inputs, there is a class of quantum computers with access to only one mixed state accompanied by n maximally mixed qubits. This model of computation is known as DQC1, or Deterministic Quantum Computation with One quantum bit, and was introduced in 1998 by E. Knill and R. Laflamme [KL98]. This model of computation is often misnamed the *one clean qubit* model, as only one qubit is polarized away from the maximally mixed state. This name is misleading, however, as it might be misconstrued that the single qubit must be pure, when in fact, even a highly mixed qubit can be used, which we will see below.

The initial state of our system is

$$\rho_i = \left(\frac{1-\alpha}{2}I + \alpha|0\rangle\langle 0|\right) \otimes \frac{I^{\otimes n}}{2^n} = \frac{1}{2^{n+1}}\begin{pmatrix}(1+\alpha)I^{\otimes n} & 0\\ 0 & (1-\alpha)I^{\otimes n}\end{pmatrix}, \tag{2.26}$$

where α is the polarization. If the first qubit was a pure state, then the polarization would be one. As we can see in Figure 2.2, the top register consists of a singe qubit in a mixed state, accompanied by n qubits in the completely mixed state. The algorithm involves

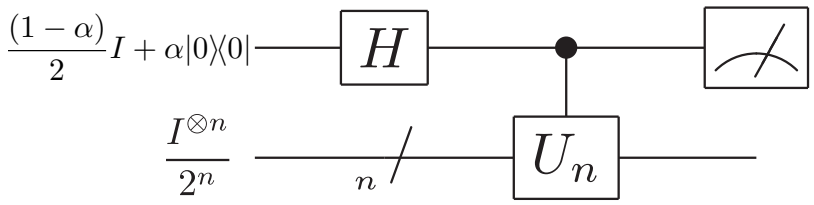

Figure 2.2: This circuit diagram depicts the DQC1 model of computation, where the first qubit is in a mixed state that has a polarization α, while the n additional qubits are in the maximally mixed state. After a Hadamard on the first qubit and a controlled unitary, a measurement is performed on the top register. By measuring the expectation value of σ_x and σ_y, the trace of the unitary is determined, which is a problem with no known efficient classical algorithm. The trace of the unitary is scaled by the number of qubits in the system and the value of the polarization of the first qubit, seen in Eqn. (2.28) and (2.29).

performing a Hadamard operation on the top register and a unitary on the bottom n qubits, controlled by the top qubit. The only requirement on the unitary is that it have an efficient decomposition into a complete set of one and two-qubit gates [BBC$^+$95, DiV95]. After the controlled-unitary U_n, the state of the system is of the form

$$\rho_f = \frac{1}{2^{n+1}} \begin{pmatrix} I^{\otimes n} & \alpha U_n^\dagger \\ \alpha U_n & I^{\otimes n} \end{pmatrix}. \tag{2.27}$$

By measuring the expectation values of the Pauli operator σ_x, you find

$$\begin{aligned} \langle \sigma_x \rangle &= \mathrm{Tr}(\rho_f \sigma_x) = \frac{\alpha}{2^{n+1}} (\mathrm{Tr}(U_n) + \mathrm{Tr}(U_n^\dagger)) \\ &= \frac{\alpha}{2^n} \mathrm{Re}(\mathrm{Tr}(U_n)) \end{aligned} \tag{2.28}$$

and similarly, a measurement of $\langle \sigma_y \rangle$ will result in

$$\begin{aligned} \langle \sigma_y \rangle &= \mathrm{Tr}(\rho_f \sigma_y) = \frac{\alpha}{2^{n+1}} (\mathrm{Tr}(U_n) - \mathrm{Tr}(U_n^\dagger)) \\ &= \frac{\alpha}{2^n} \mathrm{Im}(\mathrm{Tr}(U_n)). \end{aligned} \tag{2.29}$$

Regardless of whether the first qubit is pure or mixed, the DQC1 model of computation gives a method for determining the trace of a unitary, which is a problem that cannot be

efficiently solved with current classical algorithms. In order for the DQC1 model to be implemented in a scalable manner, the unitary must have an efficient decomposition in one and two-qubit gates. Note that even in this case, and efficient algorithm for estimating the trace is still not known.

DQC1 is an excellent computational model for implementation in NMR. One reason is that the expectation values of σ_x and σ_y are easily measured in the NMR architecture. Also, the thermal state in NMR is perfect for the initial state of the DQC1 algorithm. Recall that the (unnormalized) thermal state in NMR can be approximated to $I + \epsilon \sum_i Z_i$. In order to convert this into the DQC1 initial state we need to kill the polarization on qubits 2 through n. To do this we rotate them into the $x-y$ plane, and then apply a gradient to the magnetic field. This kills the polarization of these qubits by randomizing their phase and we are left with polarization on only the first qubit. This method is used to initialize the NMR qubits for each DQC1 experiment in this thesis.

2.2 Quantum correlations

In addition to mixed-state quantum computation, the concept of quantum correlations plays a dominant role in this thesis. In this section we will describe two different types of quantum correlations. The first is entanglement, which is easily the most well-known form of quantum correlations. It is often (incorrectly) credited as being an indicator of quantum systems: you will often hear the terms *entanglement* and *quantum* used interchangeably. While this is clearly a conflation of terms, it is easy to see why this happens: entanglement is counterintuitive to our classical experience and has proven to be a powerful resource in some protocols. For example, after years of being a staple in the science fiction world, quantum teleportation is a physical reality because of the ability to manipulate entangled systems with high fidelity control. After discussing entanglement, we will explain the second measure of non-classical correlations called quantum discord – a measure that features prominently in this thesis.

2.2.1 Entanglement

Entanglement is very important in the field of quantum information. In fact, it has been shown that an algorithm with access to pure states can be simulated classically to within

a certain tolerance, if there is less than a 'suitable small amount' of global entanglement present [JL03, Vid03]. We also know that quantum channels that do not preserve entanglement can be simulated classically [HSR03], and in quantum key distribution, a necessary condition for security is that there be entanglement verified in the effectively distributed state [CLL04].

A bipartite pure state in the Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, is said to be entangled if it cannot be written in the form $|\psi_A\rangle \otimes |\psi_B\rangle$. This means that you cannot completely describe an entangled system by providing a state vector to each subspace individually, but rather, it requires a description of the system as a whole. Important examples of this are the Bell states, one of which is shown below:

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.30}$$

There is no possible way to write $|\psi_+\rangle$ as $|\psi_A\rangle \otimes |\psi_B\rangle$, so we say it is entangled.

An entangled mixed state is one that cannot be written in the separable form

$$\rho_{AB}^{sep} = \sum_i p_i \rho_A^i \otimes \rho_B^i, \tag{2.31}$$

where $\{p_i\}$ is a probability distribution and ρ_A^i, ρ_B^i are density operators on system A and B respectively. The state given in Eqn. (2.31) is the most general state that can be created with local operations and classical communication (LOCC). In other words, it is not possible to create an entangled state by using only LOCC and starting with a separable state. Because separable states can be created using LOCC, the pervasive understanding is that these states are *classical* in nature. This is not the case, and is an oversimplification of the notion of *classical* and *quantum*. Please note that the concepts of *classical* and *quantum* are very esoteric, and have not yet been concretely defined in this thesis. We will precisely define what we mean by them in Section 2.2.2.

Entangled pure states are instrumental to many protocols, such as teleportation (first discovered in 1993 [BBC$^+$93]). Teleportation is the transferring of a quantum state from one location to another, without having it travel through the space in between. To accomplish this feat, one entangled Bell pair (like the one in Eqn. (2.30)) and two bits of classical communication are required. The protocol can be seen in Figure 2.3. Alice has an unknown qubit she wants to send to Bob, but she does not have a quantum channel available to send it. However, her and Bob share a Bell state. By taking her portion of the

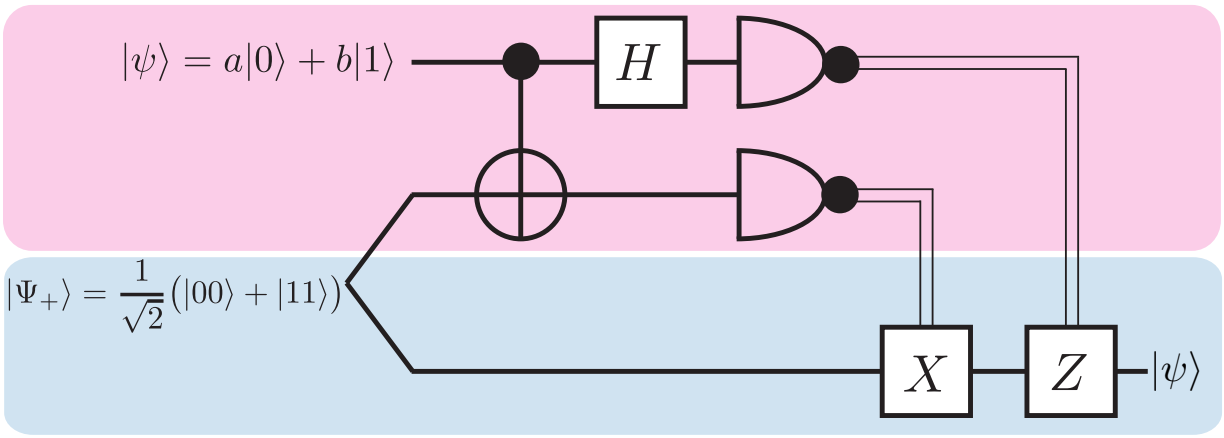

Figure 2.3: This circuit diagram depicts the teleportation protocol where Alice (the top pink block) has an unknown quantum state she wishes to send to Bob (the bottom blue block). Alice and Bob share an entangled Bell state and have the ability to send two classical bits between them, denoted by double lines in the circuit). By performing a Bell measurement on her qubits and then sending the measurement result to Bob, Alice is able to transform Bob's portion of the Bell state into the qubit she wanted to send – up to a unitary transformation. The unitary Bob needs to perform on his qubit is dictated to him by the two bits of classical communication Alice sent.

Bell state and the unknown qubit and performing a Bell measurement, she can transform Bob's portion of the Bell state into the unknown qubit, up to a unitary transformation that can be communicated classically. A Bell measurement on two qubits is equivalent to performing a controlled-not gate followed by a Hadamard on the control qubit, then measuring both qubits in the computational basis. Alice then communicates the outcome of her measurement to Bob via a classical channel, and Bob uses this information to perform the necessary unitary on his qubit to transform it into the one Alice wished to send (Alice and Bob pre-communicated which operations correspond to which measurement outcomes). By performing this procedure, Alice is able to transmit a quantum state to Bob without it ever existing in the space between them, all that was required were two bits of classical communication (one for each measurement outcome) and an entangled pair of qubits. This is surprising, since in order to completely specify a qubit, three real numbers are required, which require infinite resources to specify accurately. But, by utilizing the strong correlations present in an entangled pair, it is possible to teleport the state with only two bits of classical information!

Entanglement in mixed state computation

Entanglement is certainly a very interesting and, at times, counterintuitive feature of quantum mechanical systems. Let us look at how entanglement features in the two examples of mixed-state quantum computation mentioned in Section 2.1: NMR and DQC1.

- NMR: Recall that states in NMR are of the form

$$\rho_{NMR} = \frac{1-\alpha}{2^n} I + \alpha \rho_{pps}.$$

  It has been shown that states of this form are always separable when the polarization α obeys the relation [BCJ$^+$99]

$$\alpha \leq \frac{1}{1+2^{2n-1}}, \tag{2.32}$$

  where n is the number of qubits. The experimental results in this thesis are for four qubits, indicating that the states generated in NMR do not have entanglement if the polarization is less than or equal to $1/(1+2^7) = 7.75 \times 10^{-3}$. The initial states of the four qubit DQC1 experiments in this thesis have a polarization of $\mathbb{B}/2 = 1.46 \times 10^{-5}$,

therefore we can confirm that there is never any entanglement in these experiments. This is one of the reasons that have prompted some researchers to conclude that NMR is not actually performing any genuine quantum task. However, in an article where Braunstein et al. show that most NMR computations are done without any true entanglement, they close with the assertion that "much more needs to be understood about what it means for a computation to be a *quantum* computation"[BCJ+99]. Indeed, it is now generally understood that entanglement is not the only signature of quantum systems.

- DQC1: One of the most interesting features of the DQC1 model is that it is separable between the first and remaining n qubits at every point in the algorithm. This indicates that there is no bipartite entanglement along this splitting, even when the top register has a polarization of one and starts in a pure state. In fact, Datta et al. showed that there is very little bipartite entanglement across any splitting in the DQC1 model for a random unitary [DFC05]. Specifically, they showed that when $\alpha > 1/2$, there is a family of unitary matrices such that for any bipartite division within the bottom register there exists an amount of bipartite entanglement that is independent of the number of qubits in the system. They also show that for all unitaries and bipartite splittings, the entanglement is bounded above by a function of the polarization only, indicating that as the number of qubits in the system grows, the fraction of possible entanglement per qubit shrinks.

  When E. Knill and R. Laflamme introduced the DQC1 model of computation, they were motived by the question: "Where does the apparent power of quantum computers come from?" [KL98] Thirteen years after the creation of the DQC1 model, it still appears to offer an advantage over classical methods, and the results mentioned above [DFC05] have invoked more questions than it answered. In recent years, the thought has been that perhaps other non-classical correlations, above and beyond entanglement, are better suited to capture the apparent power of mixed state quantum computation.

Entanglement Witnesses

There are several ways to measure the bipartite entanglement present in a system (negativity [ZHSL98, VW02] and concurrence [HW97, Woo98] are two examples) – but common

among all measures is the necessity for full knowledge of the state. Acquiring the information required to reconstruct the state of a physical system is a process called tomography and it is not scalable. By this we mean that the number of resources required grows exponentially with the size of the system: for n qubits, $(4^n - 1)$ parameters need to be estimated. In order to solve this problem, *entanglement witnesses* [HHH96, Ter00] have been created. A witness is an observable that characterizes the set of separable states and allows experimentalists to physically detect entanglement with only a few measurements. The operator W is defined to be an entanglement witness if it has at least one negative eigenvalue and $\langle\psi_A|\langle\phi_B|W|\psi_A\rangle|\phi_B\rangle \geq 0$ for all pure product states $|\psi_A\rangle$ and $|\psi_B\rangle$. Once W is established as an entanglement witness, entanglement is detected in state ρ by witness W if

$$\mathrm{Tr}(W\rho) < 0. \tag{2.33}$$

Figure 2.4 abstractly depicts the set of entangled states that can be detected by witness W and those that it cannot discriminate from separable states. It is also clear from the figure that while $\mathrm{Tr}(W\rho) < 0$ witnesses entanglement, $\mathrm{Tr}(W\rho) > 0$ does not indicate that a state is separable. Different entanglement witnesses will witness entanglement for a different set of states and can be used in combination to improve the probability of successful detecting entanglement.

The introduction to entanglement presented here is by no means complete, as I have only mentioned the aspects that are important for the remainder of this thesis. The interested reader is directed to Ref. [HHHH09] for a thorough review.

Entropic quantities

Entropic quantities will be very important when we discuss quantum discord in the next section, so it is valuable to discuss these properties in the context of entanglement first. For more information, a good reference for classical information theory is Ref. [CT06]. The Shannon entropy is defined as

$$H(X) = -p_i \log p_i, \tag{2.34}$$

where $\{p_i\}$ is a probability distribution and the logarithms in this thesis are always taken to be base 2. The entropy is a measure of the uncertainty in a random variable X. For instance, think about the roll of a die and the toss of a coin – we are more uncertain about the outcome of the die than of the coin, because there are more equally probable outcomes.

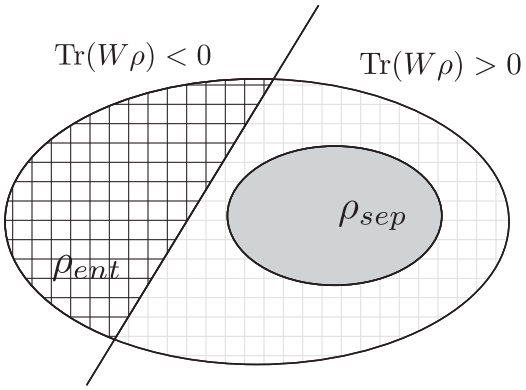

Figure 2.4: The line in this image depicts the entangled states that a particular entanglement witness W is able to detect (those to the left of the line). Note that the set of separable states are always found to have no entanglement, as ensured by the definition of an entanglement witness.

Therefore, we expect the entropy of the die to be larger than that of the coin. For the coin, there are two options, each with probability 1/2, so that the Shannon entropy is $H(X_{coin}) = -1/2 \log 1/2 - 1/2 \log 1/2 = 1$. For the roll of a dice, there are 6 possibilities, each with the probability 1/6, so the Shannon entropy is $H(X_{dice}) = 6(-1/6 \log 1/6) = \log 6 \approx 2.6$. As predicted, $H(X_{dice}) > H(X_{coin})$.

The entropy of a joint system $H(X, Y)$ has the exact same formulation, except the probability distribution is now for the joint system $\{p_{x,y}\}$. The joint entropy must be larger than or equal to the entropy of each subsystem:

$$H(X, Y) \geq H(X) \text{ and } H(Y), \tag{2.35}$$

which makes intuitive sense as adding an additional random variable to our system should not make us more certain of the outcome.

The quantum analog to the Shannon entropy is the von Neumann entropy:

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho). \tag{2.36}$$

In most situations we will not explicitly state whether we are using the von Neumann or Shannon entropy, but it should be clear from the context. For ρ with eigenvalues λ_i, the

entropy can be written as

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i, \tag{2.37}$$

where $0 \log(0)$ is defined to be zero. The entropy of a quantum system is also a measure of uncertainty, and the states that have maximal entropy are maximally mixed states

$$S(I/d) = d\left(-\frac{1}{d}\log\frac{1}{d}\right) = \log d, \tag{2.38}$$

while the minimum entropy of zero is found for pure states.

Interestingly, the inequality in Eqn. (2.35) does not hold for all quantum states, only separable (i.e. unentangled) ones. When ρ_{AB} is separable,

$$S(\rho_{AB}^{sep}) \geq S(\rho_A) \text{ and } S(\rho_B), \tag{2.39}$$

while when entangled

$$S(\rho_{AB}^{ent}) < S(\rho_A) \text{ and } S(\rho_B). \tag{2.40}$$

To illustrate this, recall that the density operator for the Bell state given in Eqn. (2.11) has reduced density matrices $\rho_A = \rho_B = I/2$, each with entropy $S(\rho_A) = S(\rho_B) = \log(2) = 1$ (remembering that all logarithms are base 2). On the other hand the Bell state has eigenvalues $\{1, 0, 0, 0\}$, giving an entropy of

$$S(\rho_{Bell}) = -1 \log 1 = 0. \tag{2.41}$$

This indicates that the Bell state has no uncertainty associated with it (there exists a measurement outcome with corresponding probability of 1), whereas its subsystems have maximal uncertainty (all measurement outcomes are equally probable).

2.2.2 Quantum Discord

While entanglement has received a lot of attention in the field of quantum information and computing, it is not the only form of non-classical correlations. Soon after the turn of the twenty-first century, the measure of quantum discord was created as a method of better capturing the non-classical correlations present in a quantum state [HV01, OZ01]. These correlations include, but are not limited to, entanglement.

The term *classical correlations* as used in current literature (and this thesis) is consistent with the idea that "classical information is locally accessible, and can be obtained without perturbing the state of the system" [OZ01]. In this sense, we can think of classical correlations as those that are insensitive to measurement. In this thesis, we define quantum correlations and non-classical correlations to be the same, defined as all correlations in excess of classical corrections. Thus, quantum correlations are sensitive to local measurements. Note that in the literature, the definition for quantum correlations is not universally agreed upon, and for that reason, I attempt to adhere to the language of 'non-classical' correlations, which tends to be less contentious. However, it is important to remember that in this thesis, there is no distinction between quantum and non-classical correlations.

Before defining quantum discord and discussing how it can help us differentiate between classical and quantum correlations, we first need to introduce the mutual information and conditional entropy. Classically, the mutual information is defined as

$$I(X:Y) = H(X) + H(Y) - H(X,Y), \tag{2.42}$$

and is a measure of how much information X and Y have in common. The relationship between different classical entropic quantities can be seen in the Venn diagram in Figure 2.5 (these relationships are the consequence of Bayes' rule). The diagram introduces another quantity, the conditional entropy. The entropy of X conditioned on knowing Y is given by

$$\begin{aligned} H(X|Y) &= H(X,Y) - H(Y) && (2.43)\\ &= \sum_y p_y \, H(X|Y=y), && (2.44) \end{aligned}$$

and can be seen directly in Figure 2.5. This value tells us how uncertain we are about X, after having measured Y. Given these definitions, it is easy to see that we can write a second, equivalent equation for the mutual information:

$$J(X:Y) = H(Y) - H(Y|X) = H(X) - H(X|Y). \tag{2.45}$$

Now, let us translate these definitions to the quantum case. The mutual information $I(X:Y)$ translates easily:

$$I_Q(A:B) = S(A) + S(B) - S(A,B), \tag{2.46}$$

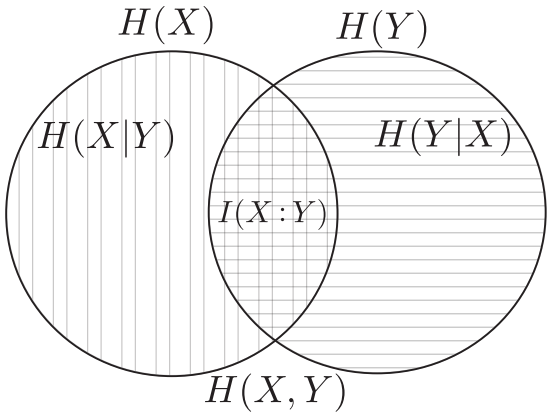

Figure 2.5: The different Shannon entropies of systems X and Y, described by classical probability distributions, are represented in the Venn diagram above. The overlapping area in the image is the mutual information $I(X:Y) = J(X:Y)$, as defined in the text.

where we are using the shorthand $S(A) = S(\rho_A)$. The problem occurs when creating a quantum analogue to $J(X:Y)$. Because the result of a quantum measurement is highly dependent on what measurement operator was used, the conditional entropy is ambiguous unless a specific measurement is indicated. By looking at the state of system B after a particular projective measurement $\{\Pi_k\}$ has been performed on system A,

$$\rho_{B|k} = \frac{\mathrm{Tr}_A((\Pi_k \otimes I_B)\rho_{AB}(\Pi_k \otimes I_B))}{\mathrm{Tr}((\Pi_k \otimes I_B)\rho_{AB}(\Pi_k \otimes I_B))} = \frac{\mathrm{Tr}_A((\Pi_k \otimes I_B)\rho_{AB}(\Pi_k \otimes I_B))}{p_k}, \tag{2.47}$$

we can define the conditional entropy for that measurement as

$$S_{\{\Pi_k\}}(B|A) = \sum_k p_k S(\rho_{B|k}). \tag{2.48}$$

It is now possible to write an expression for the quantum analogue to Eqn. (2.45),

$$J_{Q\{\Pi_k\}}(A:B) \equiv S(B) - S_{\{\Pi_k\}}(B|A), \tag{2.49}$$

where the quantum conditional entropy is a function of the measurement performed. The quantum discord is then defined as the minimum difference between the two classically

equivalent formulations of the mutual information over all possible projective measurements:

$$D(A:B) = \min_{\{\Pi_k\}}(I_Q(A:B) - J_Q(A:B)) = S(\rho_A) - S(\rho_{AB}) + \min_{\{\Pi_k\}} \sum_k p_k S(\rho_{B|k}). \quad (2.50)$$

If the quantum discord is zero, then the values for both formulations of the mutual information are equivalent and the state ρ_{AB} is said to only contain classical correlations. In this case there exists a measurement on system A that does not affect the entropy of the total system, and all correlations present can be found in purely classical systems. However, if the value of the quantum discord is greater than zero, then there exist correlations stronger than what can be found in classical systems, known as non-classical or quantum correlations.

Quantum discord is bounded from below by zero and above by the entropy of the measured subsystem, $S(A)$. The proof of this and many other properties of quantum discord are very nicely described in the doctoral thesis of Dr. Animesh Datta [Dat08] and I direct the interested reader there for more information. It is worth noting that for all pure states, quantum discord is only found to be non-zero when ρ_{AB}^{pure} is entangled. That is to say that pure, separable states contain only classical correlations, while separable mixed states, given by Eqn. (2.31), may contain non-zero discord.

Examples of States with Quantum Discord

In order to better understand the correlations captured by quantum discord, let us look at a couple of examples. The first example will illustrate the lack of symmetry in the measure of quantum discord, namely that $D(A:B)$ is not necessarily equal to $D(B:A)$. The second example looks at a Werner state and how the quantum discord behaves over the entangled/separable boundary.

1. Consider the state

$$\rho_{AB} = \frac{1}{2}\Big(|0\rangle\langle 0| \otimes |-\rangle\langle -| \; + \; |1\rangle\langle 1| \otimes |0\rangle\langle 0|\Big), \quad (2.51)$$

where $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$, which is a separable mixed state with non-zero quantum discord $D(B:A)$, although the discord $D(A:B)$ is equal to zero. This illustrates that

the quantum discord is not a symmetric measure, as it depends on which system the measurement is acting on. In this example, $D(A:B) = 0$ can be easily determined by noticing that a measurement in the computational basis on system A will not disturb the total system. In other words, there exists a measurement on system A such that the full state on $\mathcal{H}_{\mathcal{AB}}$ remains unchanged and $I_Q(A:B) = J_Q(A:B)$. On the other hand, if the measurement is being performed on system B, then any choice of measurement will disrupt the final state, indicating the presence of non-zero discord: $D(B:A) \approx 0.2$.

This example illustrates what the literature calls a classical-quantum (CQ) state. These states are defined by

$$\rho_{AB}^{CQ} = \sum_j p_j |j\rangle\langle j| \otimes \rho_j^B, \tag{2.52}$$

where $\{|j\rangle\}$ is an orthonormal basis for system A, and ρ_i^B are any density matrices on system B. Classical-quantum states have $D(A:B) = 0$ and $D(B:A) \neq 0$. Similarly, we can define quantum-classical (QC) states

$$\rho_{AB}^{QC} = \sum_j p_j \rho_j^A \otimes |j\rangle\langle j|, \tag{2.53}$$

such that $D(A:B) \neq 0$ and $D(B:A) = 0$. Finally, to complete this set of definitions, there are also states called classical-classical (CC) that have the form

$$\rho_{AB}^{CC} = \sum_{j,k} p_{jk} |j\rangle\langle j| \otimes |k\rangle\langle k|, \tag{2.54}$$

where p_{jk} is a joint probability distribution. These states are simply referred to as classical states, and as one might suppose, CC states have zero discord, regardless of what subsystem the measurement is performed on.

2. An interesting state to study is that of a maximally entangled Bell state $|\psi_+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, combined with the maximally mixed state:

$$\rho_W = \frac{(1-z)}{4} I^{\otimes 2} + z|\psi_+\rangle\langle\psi_+|. \tag{2.55}$$

This state is well known, belongs to the set of *Werner states*, and is known to be separable for $z < 1/3$. Using Eqn. (2.50), we can calculate the value of discord without much trouble. The reduced density matrix ρ_A has eigenvalues $\{\lambda_i\} = \{1/2, 1/2\}$,

and an entropy of

$$\begin{aligned} H(\rho_A) &= -\sum_i \lambda_i \log \lambda_i \\ &= -\frac{1}{2}\log\left(\frac{1}{2}\right) - \frac{1}{2}\log\left(\frac{1}{2}\right) \\ &= 1. \end{aligned}$$

The full state ρ_{AB} has eigenvalues $\{\lambda_i\} = \{\frac{3z+1}{4}, \frac{1-z}{4}, \frac{1-z}{4}, \frac{1-z}{4}\}$, giving an entropy of

$$\begin{aligned} H(\rho_{AB}) &= -\sum_i \lambda_i \log \lambda_i \\ &= -\frac{3z+1}{4}\log\left(\frac{3z+1}{4}\right) - 3\frac{1-z}{4}\log\frac{1-z}{4} \\ &= -f\log f - (1-f)\log\frac{1-f}{3}, \end{aligned}$$

where $f = (3z+1)/4$. This just leaves the conditional entropy to calculate. Luckily, the choice of measurement for this state does not change the conditional entropy, as this state is symmetric and minimization is not required. For convenience, we choose to measure in the computational basis. A measurement on system A has a probability of $1/2$ for both outcome 0 and 1. If the outcome of the measurement on system A is 0, then the state of B is

$$\rho_{B|A=0} = \begin{pmatrix} \frac{1+z}{2} & 0 \\ 0 & \frac{1-z}{2} \end{pmatrix}, \tag{2.56}$$

and when the outcome is 1,

$$\rho_{B|A=1} = \begin{pmatrix} \frac{1-z}{2} & 0 \\ 0 & \frac{1+z}{2} \end{pmatrix}. \tag{2.57}$$

In both cases, the eigenvalues are the same: $\{\frac{1+z}{2}, \frac{1-z}{2}\}$, leading to a conditional entropy of

$$\begin{aligned} H(B|A) &= \sum_i p_i H(B|A=i) \\ &= \frac{1}{2}H_2\left(\frac{1-z}{2}\right) + \frac{1}{2}H_2\left(\frac{1-z}{2}\right), \end{aligned}$$

where $H_2(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy function. The discord of the Werner state is then

$$D(\rho_W) = 1 + f\log(f) + (1-f)\log\left(\frac{1-f}{3}\right) + H_2\left(\frac{1-z}{2}\right), \tag{2.58}$$

where $f = \frac{3z+1}{4}$. Figure 2.6 is a plot of the discord as a function of z and from it one can see that the discord is non-zero, provided $z > 0$, even when there is zero entanglement. In addition, the discord is smooth over the boundary at $z = 1/3$ (where the state becomes entangled), suggesting that there is nothing significant about this boundary for the quantum correlations characterized by the quantum discord.

Quantum discord is only one of many proposals for measures of quantum correlations [HHH$^+$05, OHHH02, PHH08, Xu11, SJSD11, GPA11, WG11, MPS$^+$10, LZ09, GPW05]. In Chapter 5 we analyze the measure of geometric discord (a measure of quantum correlations defined in Ref. [DVB10]), which has some advantages over quantum discord when performing analytical calculations. While I have made every effort to cite the works on quantum correlations that are most relevant to this thesis, the articles on quantum discord and quantum correlations cited in this thesis are by no means exhaustive. When the work on discord presented in this thesis began, there were only a handful of discord papers published. Since then the number has increased dramatically, as can be seen in Table 2.1. For a more thorough treatment of recent studies on quantum discord the reader is directed to Ref. [CMS11].

Year	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Citations	4	6	3	4	3	6	15	16	67	152

Table 2.1: The number of citations that the original paper defining quantum discord [OZ01], published in 2002, has received each year as recorded by the American Physical Society (data taken from prl.aps.org on January 7, 2012).

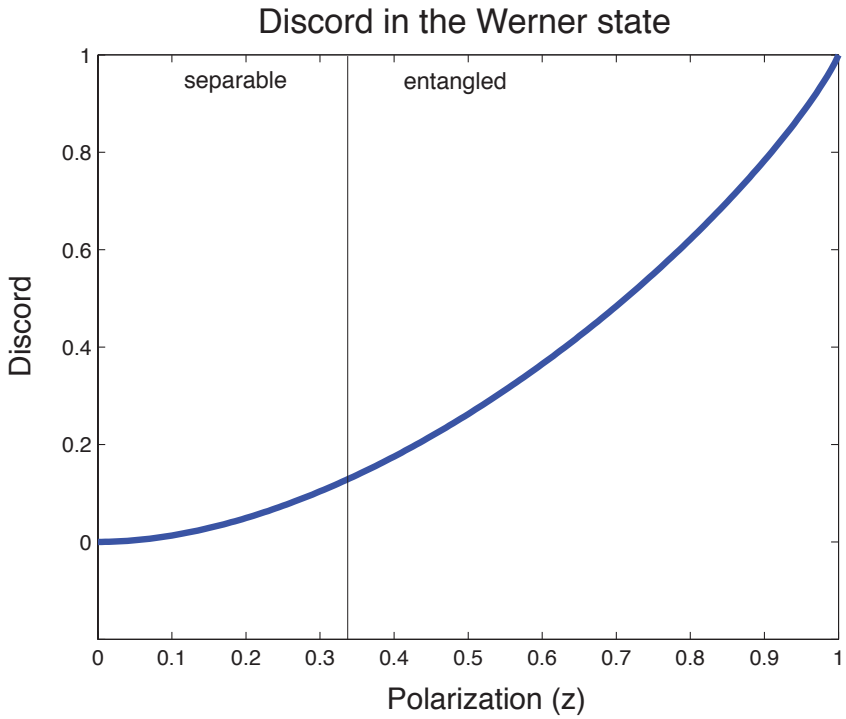

Figure 2.6: Plot of the discord in the two-qubit Werner state $\rho_W = \frac{(1-z)}{4} I^{\otimes 2} + z|\Psi_+\rangle\langle\Psi_+|$ as a function of z. The line at $z = 1/3$ divides the separable states (those on the left with $z < 1/3$) from the entangled states (those on the right with $z \geq 1/3$). One can clearly see that there are separable states that still have non-zero quantum discord. In fact, zero discord is only achieved for $z = 0$ where the state is maximally mixed.

Quantum discord mixed state computation

Now that we have a basic understanding of quantum discord, let us take a quick look at quantum discord in the two examples of mixed-state quantum computation discussed previously: DQC1 and NMR.

- DQC1: So far we have explained the DQC1 model of computation and the (lack of) entanglement contained in the model. Here we would like to give a quick snapshot at the studies done so far on discord and other non-classical correlations in DQC1. In 2007, it was shown that DQC1 contains a large amount of non-classical correlations as indicated by the operator Schmidt rank, and therefore, it was conjectured that the model is unlikely to be able to be simulated classically [DV07]. In the following year, the non-classical correlations in the DQC1 model as measured by the quantum discord were analyzed [DSC08], and it was found that the quantum discord in a typical instance of the DQC1 algorithm for a larger number of qubits (> 5) is not dependent on the number of qubits in the system, but only the polarization of the top qubit. They showed that even when the polarization of the top qubit is less than 0.5 (where it is unlikely there is any entanglement [DFC05]) there are non-classical correlations as measured by the discord. The non-classicality of the DQC1 model has also been studied in the context of local noneffective unitary operations and measurement-induced disturbance [DG09], which showed signs of non-classicality.

  The quantum discord in a two-qubit DQC1 algorithm has been experimentally measured using optical qubits [LBAW08]. In order to measure the amount of discord, full tomographic data for the final state of a DQC1 experiment was measured for input states of varying purity and used to calculate the quantum discord and entanglement. Entanglement was not detected; however non-zero values for the quantum discord was measured. Quantum discord in the DQC1 model are the main subjects of Chapters 4 and 5, and this discussion will be continued there.

- NMR: As previously mentioned, the states present in NMR quantum information processing are pseudopure states that generally have a small polarization. For instance, the experiments in this thesis are performed with a polarization of 1.43×10^{-5}, which is below the threshold for entanglement. The presence of quantum discord in an NMR quantum information processor would indicate that it is not a purely classical model, but contains quantum correlations. If we calculate the quantum discord

Name	Hamiltonian	Discord
Weak coupling	$H = \pi\omega_1 ZI + \pi\omega_2 IZ + \pi JZZ$	0
Strong coupling	$H = \pi\omega_1 ZI + \pi\omega_3 IZ + \pi J(XX + YY + ZZ)$	6.98×10^{-8}
Dipolar coupling	$H = \pi\omega_1 ZI + \pi\omega_2 IZ + \pi D(2ZZ - XX - YY)$	7.02×10^{-8}

Table 2.2: The amount of discord present in the thermal states of several Hamiltonians that arise in two-qubit NMR systems. The discord is calculated assuming a carbon-13 nuclei in a 16.7 T magnet at room temperature (ie. a polarization of 1.4×10^{-5}). Parameters used in the Hamiltonians are: $\omega_1 = 3000$, $\omega_2 = 10000$ Hz, $\omega_3 = 4000$ Hz, and $J = D = 20$ Hz.

in the Werner state from Eqn. (2.55) for our experimental polarization, we find that it is equal to 2.83×10^{-10}. This is a very small amount of discord, yet it is non-zero. Note that currently, it is not known what a given amount of discord means; that is to say that there is no known lower bound to which separates useful from unusable discord. In Chapter 4 we set out to detect a very small amount of quantum discord in liquid-state NMR.

While it has been shown that almost all quantum states contain quantum discord [FAC$^+$10], the thermal state of a weakly-coupled liquid-state NMR experiment has zero discord. However, this is not true of the thermal states of other NMR Hamiltonians. The thermal state in NMR systems is defined as

$$\rho_{th} = \frac{1}{N} e^{-\beta H}, \tag{2.59}$$

where N is the number of spins and H is the Hamiltonian of the system. In Table 2.2 we summarize the amount of discord present in the thermal states of various two-qubit Hamiltonians of interest in NMR, and as you can see, the thermal state can contain non-zero discord. Note that while the thermal state in NMR can contain non-classical correlations, the initial states for the DQC1 algorithm do not.

There have been a couple of experimental studies on the quantum correlations present in NMR systems. In Ref. [AC$^+$11] the authors measure the sudden-change in the quantum and classical correlations of two qubits in experimental NMR pseudopure states as they undergo relaxation. They also show that there are some states whose classical correlations are robust against certain noise models. In Ref. [SPCA$^+$10] they investigate the quantum correlations present in a two-qubit state using a quadrupolar

NMR system. They measured the quantum and classical correlations as well as the mutual information during decoherence. Note that in both of these cases, only the pseudopure state was accounted for, and not the physical NMR state. This is in contrast to the work in this thesis, where we concentrate on detecting and quantifying the discord present in the full quantum state.

Chapter 3

Experimentally implementing a DQC1-complete problem

In this chapter, we describe the experimental implementation of the DQC1 model of computation from Section 2.1.3. The problem solved using DQC1 is that of approximating the Jones polynomial at the fifth root of unity. The Jones polynomial is an important knot invariant which distinguishes between distinct knots, a problem that cannot be efficiently solved with current classical algorithms. The experimental implementation detailed here uses four qubits in liquid-state NMR. Our motivation for performing this particular experiment is outlined below:

- The DQC1 class of quantum computers is of great interest, primarily due to their ability to solve a problem with no known efficient classical algorithm, despite possessing limited entanglement (as discussed in Section 2.2.1). In addition to being a problem that can be solved efficiently on the DQC1 class of quantum computers, approximating the Jones polynomial has been shown to be a *complete problem* for DQC1. In other words, any problem that can be solved using DQC1 can be reduced to the problem of solving for the Jones polynomial. Our experiment is the first experimental implementation of a DQC1-complete algorithm.

- This algorithm relies on the ability to differentiate experimental outcomes with great accuracy. It has recently been shown that in liquid-state NMR, single-qubit gates can be performed with an average error per gate of $1.3 \pm 0.1 \times 10^{-4}$ [RLL09], and this level

of control, if applied to a four-qubit experiment, such as the one presented in this chapter, would be exceptional. However, note that this average fidelity is for pulses that perform single-qubit gates on a single-qubit molecule, and have a total length of 516.8μs. Meanwhile, for the more complicated unitary transformations required in this experiment, the gates require approximately 60ms, and as such, will have lower average fidelity. In addition, when generalizing the benchmarking experiment to multi-qubit gates, the average fidelity decreased by a factor of 10 for three qubits (the set of gates used were single qubit rotations and CNOT gates between pairs of qubits). The length of this experiment, and the precision required by the algorithm in order to successfully distinguish distinct knots, make for a difficult experiment, that pushes the boundary of our current level of control.

- The Jones polynomial is a quantity that has a broad application across many fields in physics – including quantum gravity, particle theory, quantum field theory, statistical physics, and applied mathematics [Kau91]. A quantum algorithm that can approximate the Jones polynomial and be implemented in a physical system is most certainly of interest to the broad physics community.

The Jones polynomial is an important tool that is used for distinguishing knots. Given two knots, it is very difficult to determine whether they are topologically distinct. Even the simplest possible instance of this problem, distinguishing a knot from an unknotted loop (fittingly called the *unknot*), is extremely difficult and is known to be in the complexity class NP [HLP99]. (Note that in this introduction we mention several different complexity classes only to indicate the comparative difficulty of certain tasks; the interested reader is directed to Ref. [KLM07] for a comprehensive introduction to the topic, one that we do not attempt in this thesis.) The problem of determining whether two knots are equivalent can easily be understood using common experience: imagine being given a necklace that has been tangled into a knotted mess and being asked if it is possible to untangle it without undoing the clasp. This is precisely the problem of distinguishing a knot from the unknot.

In order to assist in differentiating knots, mathematicians have created a mathematical tool called the knot invariant [Kau88]. Knot invariants have different values for knots that are not equivalent; in other words, if a knot invariant evaluates to different values for two knots, they are guaranteed to be distinct. One of the most important knot invariants is called the Jones polynomial, and was discovered in 1984 by Vaughan Jones [Jon85]. It improves on previously discovered knot invariants, such as the Alexander polynomial [Ale28],

in its ability to distinguish *oriented* knots; in other words, it can distinguish between a knot and its mirror image.

While the Jones polynomial is of great benefit to the field of knot theory, using it to solve practical problems is not efficient as exact evaluation of the Jones polynomial at all but a few points is hard for the complexity class #P [JVW90]. Quantum algorithms for evaluating the Jones polynomial have been attempted and approximations at several special points have been shown to be complete for the complexity class BQP [FKW02, FLW02]. Building on this work, it was then shown that approximations of the Jones polynomial at principal roots of unity can be computed on a quantum computer in polynomial time [AJL06], later being shown that for certain closures the problem is BQP-complete [AA11, WY08]. The algorithm developed by P. Shor and S. Jordan shows that approximating the Jones polynomial at the fifth root of unity for any knot is a complete problem for DQC1 [SJ08]. It is this algorithm that is modified for implementation in NMR, and is the focus of this chapter.

There has been one other study on solving the Jones polynomial using quantum information processors: an algorithm that can solve the Jones polynomial for three strand braids [KJ07] was implemented in NMR on two qubits for the specific cases of the trefoil knot, the figure-eight knot, and the Borromean rings [MFK$^+$10]. The fundamental difference between the work presented in this chapter and the experiment implemented in Ref. [MFK$^+$10], is that the latter only applies to knots whose braid representations have three strands, while ours can be extended to any size knot without changing the computational complexity.

This chapter describes the first experimental implementation of a complete problem for the DQC1 model of quantum computation. The implemented algorithm is a modification of the algorithm developed by P. Shor and S. Jordan [SJ08] that is suitable for implementation in NMR. The experimental findings have been published in Physical Review Letters [PMRL09], copyright (2009) by the American Physical Society. The author of this thesis performed the entirety of the experiment with guidance from C.A. Ryan and modified the original algorithm and jointly analyzed the data with O. Moussa.

The first section of this chapter begins with a discussion of the relevant components of knot theory that lead us to the definition of the Jones polynomial, which is evaluated for the trefoil knot as an explicit example. Fibonacci particles, required for the construction of the algorithm used, are explained in Section 3.2, and our modified algorithm is described

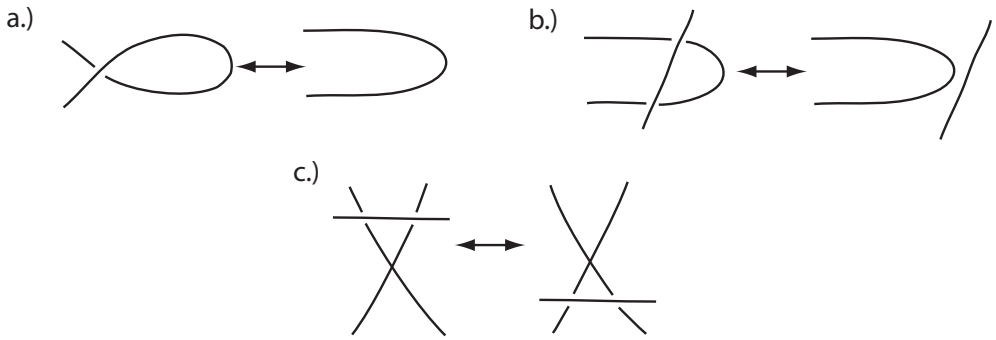

Figure 3.1: These three manipulations are called the *Reidemeister moves* and do not change the topological properties of a knot. If one knot can be transformed into another using only Reidemeister moves, the two knots are said to be topologically equivalent, up to ambient isotopy.

in Section 3.3. Finally, the experimental implementation is detailed in Section 3.4 with the results and a discussion in Section 3.5.

3.1 Knots, Braids, and the Jones Polynomial

3.1.1 Knots

The mathematical definition of a knot is the embedding of a circle in $\mathbb{R}^3$, and can easily be understood by imagining a knotted rope or string. More than one circle embedded in $\mathbb{R}^3$ is a link. For our purposes it is not important to distinguish between links and knots and we will refer to both as knots throughout this chapter. When it is said that two knots are equivalent, we are referring to their topology. Technically, two knots are said to be equivalent up to ambient isotopy, which means that two knots are topologically equivalent if you can manipulate one (non-oriented) knot into the other without breaking any of the strands. More specifically, flipping a knot around any axis is not permitted as this changes the topological properties of oriented knots. In other words, an oriented knot and its mirror image are not necessarily topologically equivalent. Mathematically, the permitted motions are referred to as the three *Reidemeister moves*, which can be seen in Figure 3.1. The

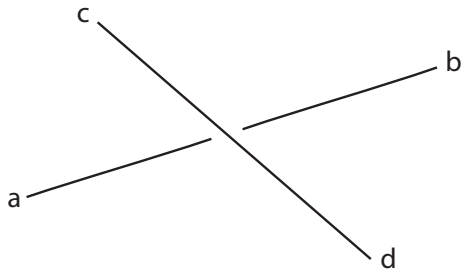

Figure 3.2: The line 'cd' is crossing over the line 'ab', as indicated by the break in line 'ab'.

more complicated the knot, as measured by the number of strands and crossings, the more difficult it is to distinguish. There quickly becomes a point where topologically equivalent knots appear vastly different and manipulating them using Reidemeister moves becomes impractical. In these situations, knot invariants are an essential tool.

Mathematically, knots are represented by characterizing their crossings. The depiction of a single crossing in Figure 3.2 is understood as strand 'cd' crossing over strand 'ab'. Constructing the Jones polynomial requires us to define the action of splicing such a crossing, which is the action of removing the crossing by cutting the strands (leaving four open ends) and fusing them together in order to create an avoided crossing. An individual crossing can be spliced in two different ways, called the A and B splice, and are depicted in Figure 3.3. In order to differentiate between them, we need to define the regions around a crossing. When looking at a single crossing there are four regions, labeled as follows: if you are approaching a crossing along the strand traveling underneath, the A region is on your left and the B region is on your right. Then the A splice is defined so that it connects the two A regions, and the B splice connects the B regions.

Now that we have the ability to deconstruct a crossing, we can use this to deconstruct an entire knot. In doing so, we will create a tree of descendants, all the while keeping track of the types of splicing used. We are interested in the primitive, or final descendants, and the types of splicings used to create each descendant. In Figure 3.4 we can see the eight primitive descendants of the trefoil knot. Note that if a knot has n crossings, then it will have 2^n descendants. (The trefoil knot, shown in Fig. 3.8 has three crossings and $2^3 = 8$ primitive descendants.) The primitive descendants of a knot K are called the *states* of K and are denoted σ. (Apologies for the duplicate notation with the Pauli

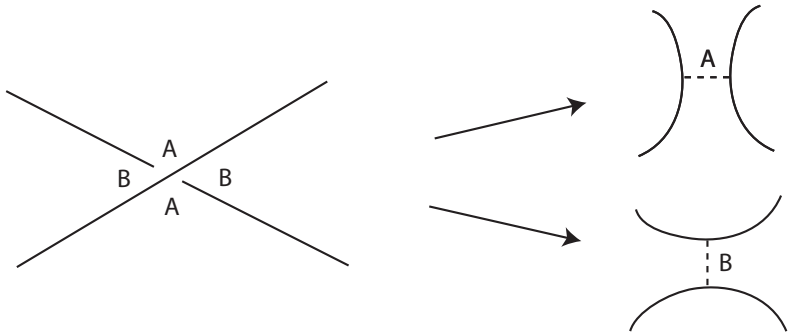

Figure 3.3: The A (B) region is defined as the region that is to your left (right) when approaching a crossing along the strand that travels underneath. The A and B splicings connect the A and B regions, respectively.

matrices. The states of K feature only briefly in this chapter and therefore we will stick with the conventional notation.) After defining the states of K, the bracket[1] $\langle K|\sigma\rangle$ can be introduced, which is a product of the splicing types that were used to construct σ. An example of a bracket for the trefoil knot that was deconstructed in Figure 3.4 is given in Figure 3.5. We can also define the norm of state σ as $||\sigma||=$ (number of loops – 1). So the norm of the state σ given in Figure 3.5 is $||\sigma|| = 3 - 1 = 2$.

[1]The bracket in knot theory has no relation to the bra-ket notation used in quantum theory, and only features briefly in this chapter. Apologies again for the duplicate notation.

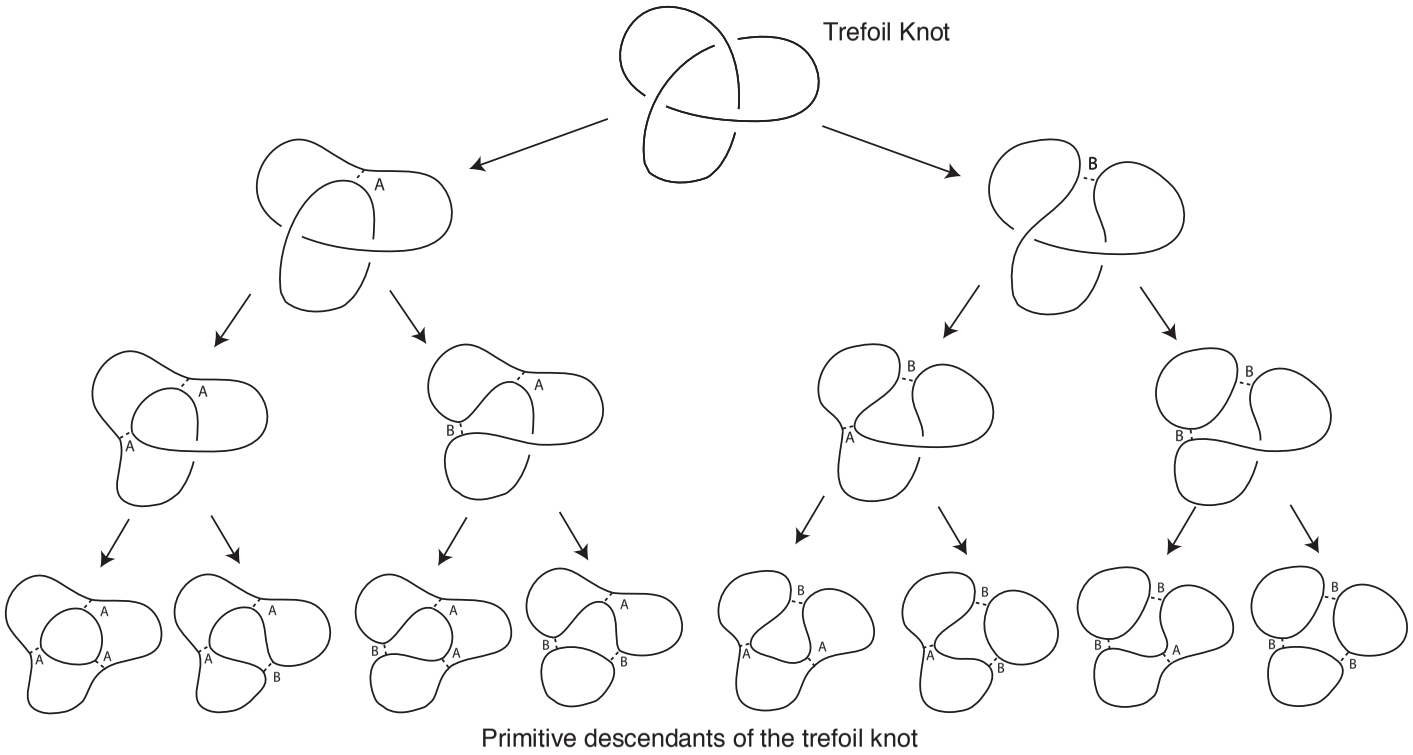

Figure 3.4: The eight primitive descendants of the trefoil knot are shown in this family tree. The location of each splice is indicated with a dotted line and labeled with the type of splice used.

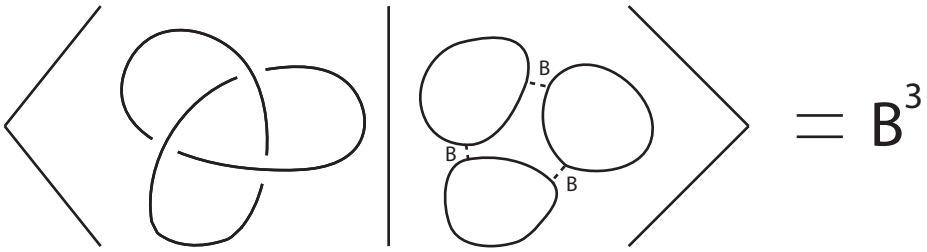

Figure 3.5: The bracket $\langle K|\sigma\rangle$ for a descendant of the trefoil knot where σ is the state which was arrived at by three B splices.

3.1.2 Braids

In this section, we explain the *braid representation* of a knot, which is important in order to understand the algorithm for approximating the Jones polynomial in DQC1. Braids are composed of N strands that cross over and under each other, and can be seen in Figure 3.6. When illustrating a braid, the top is the beginning and the bottom is the end.

Braids are comprised of elementary crossings[2], σ_i, each of which is simply a single crossing of strand i over strand $i+1$. For an n-strand braid there are $n-1$ elementary crossings and their $n-1$ inverses, where the inverse, σ_i^{-1}, is strand $i+1$ crossing over strand i. These $2(n-1)$ elementary crossings generate the braid group $\mathbb{B}_n$. Multiplication in the braid group is performed by attaching the bottom strands of one braid to the top strands of another. Elementary crossings satisfy the following conditions:

$$\sigma_j\sigma_j^{-1} = 1 \tag{3.1}$$

$$\sigma_j\sigma_k = \sigma_k\sigma_j \text{ for all } |j-k|>1 \tag{3.2}$$

$$\sigma_j\sigma_{j+1}\sigma_j = \sigma_{j+1}\sigma_j\sigma_{j+1} \text{ for all } j. \tag{3.3}$$

The second condition, Eqn. (3.2), is pictorially demonstrated in Figure 3.6.

Braids are related to knots by their "closure". In fact, every knot can be represented as the trace closure of a braid. The trace closure, as illustrated in Figure 3.7, connects

[2]Once again, apologies for the duplicate notation. Unfortunately, the elementary crossing feature prominently in this chapter, so the Greek letter sigma will always refer to elementary crossings throughout the chapter.

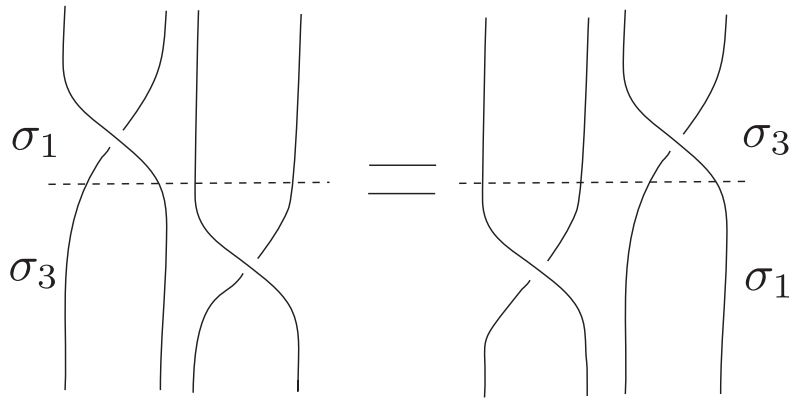

Figure 3.6: Pictorially demonstrating the condition $\sigma_j\sigma_k = \sigma_k\sigma_j$ for all $|j-k| > 1$ where $j = 1$ and $k = 3$, in a four strand braid.

the top of each strand to the bottom in order to transform the braid into a knot or link. The right most strand at the top of the braid is connected to the right most strand at the bottom, and the second right most strand at the top is connected to the second right most strand at the bottom, and so on until all the strands have been connected. This can be done by adding n uncrossed strands to an n-strand braid and connection the tops and bottoms as seen in Fig. 3.7.

With the braid representation comes the notion of the orientation of a knot. The orientation of a knot can be thought of as the direction of the rope, as can be seen in Figure 3.8. The convention is that when closing a braid, the direction of the strand goes from the bottom to the top. Now that we have defined the orientation of a knot, it is possible to define positive and negative crossings, as shown in Figure 3.9, and the *writhe* of a knot. The writhe, $w(K)$, is the number of positive crossings minus the number of negative crossings in an oriented knot. The oriented trefoil knot in Fig. 3.8 has three positive crossings, therefore $w(\text{trefoil}) = 3$. Note that elementary crossings σ_i correspond to negative crossings, and elementary crossings σ_i^{-1} correspond to positive crossings.

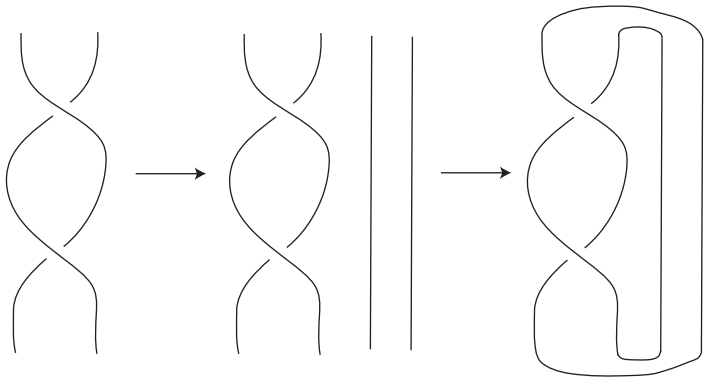

Figure 3.7: The braid on the left undergoes the trace closure to become the knot on the right. The trace closure is performed by taking the number of strands in the braid, adding that number of uncrossed strands to the side of the braid (shown in the middle step) and connecting the top of each new strand to the top of the corresponding braided strand, and likewise for the bottoms.

3.1.3 Jones polynomial

We now have all the basic information needed to compose the equation for the Jones polynomial, which we will explicitly find for the trefoil knot, pictured in Figure 3.8. We begin by defining the bracket polynomial as

$$\langle K \rangle = \sum_{\sigma} \langle K|\sigma\rangle d^{||\sigma||}, \tag{3.4}$$

where σ runs over all the primitive descendants of K. Recall that the bracket $\langle K|\sigma\rangle$ is a product of the splicings used to decompose knot K into primitive descendent σ. The trefoil knot has a bracket polynomial of

$$\langle \text{trefoil} \rangle = A^3 d + 3A + 3A^{-1} d + A^{-3} d^2. \tag{3.5}$$

The bracket polynomial itself is not a knot invariant, but by enforcing $B = A^{-1}$ and $d = -A^2 - A^{-2}$, the bracket polynomial becomes invariant under the second and third Reidemeister moves. This simplifies the polynomial in Eqn. (3.5) to $\langle \text{trefoil} \rangle = A^{-7} - A^5 - A^{-3}$. The polynomial can become invariant over the final Reidemeister move by

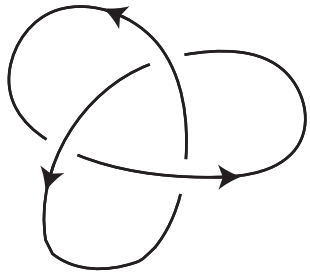

Figure 3.8: Oriented trefoil knot. These three crossings are all positive, and give the knot a writhe of $w = 3$.

normalization to create the "f-polynomial":

$$f_K(A) = (-A^3)^{-w(K)}\langle K\rangle. \tag{3.6}$$

The writhe of the oriented trefoil knot is given in Figure 3.8 is 3, leading to the f-polynomial:

$$f_{\text{trefoil}}(A) = -A^{-16} + A^{-4} + A^{-12}. \tag{3.7}$$

From here it is straightforward to define the Jones polynomial, $V_K(t) = f_K(t^{-1/4})$. Therefore, the oriented trefoil knot has a Jones polynomial of

$$V_{\text{trefoil}}(t) = t + t^3 - t^4. \tag{3.8}$$

We are able to compose the Jones polynomial for simple knots with very few crossings, but since the number of descendants grows exponentially with the number of crossings in the knot, this method is not scalable. In fact, there is no known scalable method for composing the Jones polynomial of a knot. There are, however, methods using quantum information processing devices for approximating the Jones polynomial at the fifth root of unity, as referenced in the introduction to this chapter.

3.2 Fibonacci Particles

In order to understand the algorithm for evaluating the Jones polynomial in DQC1, we must first explain Fibonacci particles, which is done in the context of the Temperley-Lieb

Figure 3.9: Definition of the positive and negative oriented crossings. A positive crossing is defined as the left strand crossing over the right, when you are traveling along the direction of the strand. While the negative crossing is defined as the right strand crossing over the left.

recoupling theory, following the route taken in Ref. [KL07]. However, the intricacies of this theory are not important for the material presented in this chapter, so we only describe the Fibonacci particles in a manner that will allow us to arrive at a unitary representation of the braid group, whose trace is related to the Jones polynomial at a particular point. (The explanatory route taken in this section follows the simplistic approach to the material given in Ref. [SJ08].)

Fibonacci particles [KL07] are purely mathematical objects that can exist in two states, marked (p) and unmarked ($*$). For our purposes, the most important aspect of Fibonacci particles are the rules they obey during interactions. Two marked particles can interact to result in either a marked, or an unmarked particle. A marked and unmarked particle always interact to create a marked particle, and two unmarked particles never interact in this theory. These interaction rules are depicted in Figure 3.10 using tree diagrams.

The algorithm is constructed by making use of the different interaction pathways that n marked particles can undergo to result in an unmarked particle. The different pathways form a basis that allow us to discuss a connection between unitary operations and braiding operations, which we will explain below. For example, let us look at the different pathways that four marked particles can undergo to result in an unmarked particle. This is most easily seen graphically using several left-associated tree structures that have marked particles at the top and one unmarked particle at the bottom. Figure 3.11 shows the tree diagrams for the two different pathways. In this case, it can be seen that there are two different paths, which represent the two basis vectors, p and $*$, in the complex vector space

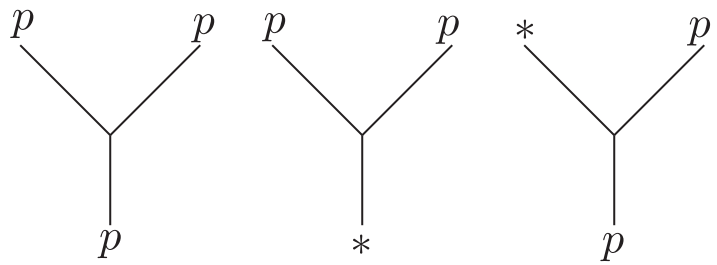

Figure 3.10: Tree diagrams showing the interaction rules for two Fibonacci particles. The rules indicate that two marked (p) particles can interact to give a marked particle or an unmarked particle ($*$), while a marked particle and an unmarked particle always interact to give a marked particle, and two unmarked particles never interact.

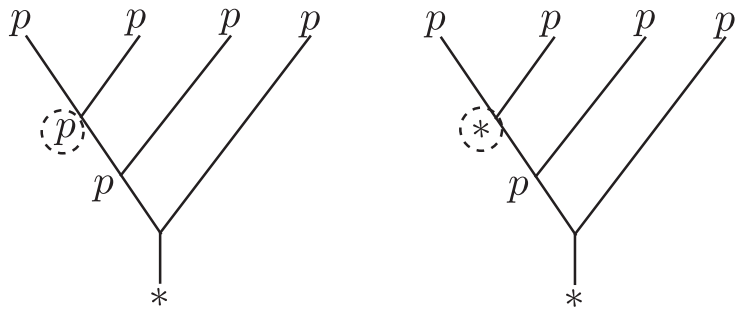

Figure 3.11: The complex vector space $V_0^{(4)}$, has basis vectors p and $*$ which can be found by creating a left-associated tree diagram with 4 marked particles at the top and an unmarked particle on the bottom. The differences in the paths are indicated by a dotted circle and indicate the basis vectors.

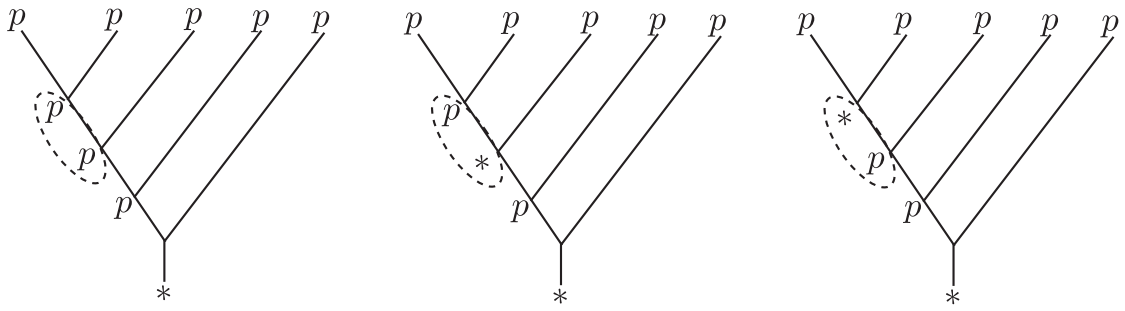

Figure 3.12: The complex vector space $V_0^{(5)}$, has basis vectors pp, $p*$, and $*p$ that can be found by creating a left-associated tree diagram with 5 marked particles at the top and an unmarked particle on the bottom. The differences in the paths are indicated by a dotted circle and correspond to the basis vectors.

$V_0^{1111} = V_0^{(4)}$. In this notation the ones on the superscript indicate the number of marked particles on the top of the tree, and the zero in the subscript indicates that an unmarked particle is at the bottom of the tree. This vector space has dimension $dim(V_0^{(n)}) = f_{n-1}$, where $f_k = [1,\ 1,\ 2,\ 3,\ 5,\ 8,\ \ldots]$ is the Fibonacci sequence. In this example where $n = 4$, the dimension of the space is 2.

For a tree with five marked particles at the top, there are three different paths leading to the unmarked state at the bottom (seen in Figure 3.12), and these three paths are the three basis vectors in the 3-dimensional vector space, $V_0^{(5)}$. Notice that the resulting f_{n-1} basis vectors contain every possible combination of p and $*$ with the restriction that there are no two unmarked particles side by side. It is possible to separate the basis vectors of the vector space $V_0^{(n)}$ into four subspaces: the vectors that start with p and end with p, start with p and end with $*$, start with $*$ and end with p, and finally, those that start and end with $*$. These subspaces are important for our purposes as we only encode two of them (the f_{m-1} vectors of the form $*\ldots p$ and the f_{m-2} vectors of the form $*\ldots*$, where m is the number of elements in the basis vectors) for use in formulating the algorithm.

We are able to map the subset of Fibonacci basis vectors of interest to computational basis vectors that are suited for our computation by a Zeckendorf representation (z-representation), which decomposes a whole number into a sum of non-consecutive Fibonacci numbers. In order to do this we will label our m-element basis vectors $s_m s_{m-1} \ldots s_1$

and let p correspond to 0 and $*$ correspond to 1. The original algorithm [SJ08] uses the z-representation of $z(s) = \sum_i s_i f_{i+1}$. To allow for better implementation with the experimental constraints we are working with, we modified the algorithm by changing the Zeckendorf representation to be

$$z' = 2^{b-1} s_1 + \sum_{i=2}^{m-2} s_{i+s_1} f_i, \tag{3.9}$$

where m is the number of elements in our basis vectors, which will correspond to $N = m-1$ strands in the braid, and $b = \lceil \log_2 f_{m-1} \rceil + 1$, which corresponds to the number of qubits required for our algorithm. As mentioned in the previous paragraph, we only convert those basis vectors that start with $*$. This modification of the algorithm changes not only the final expression for the Jones polynomial, but the DQC1 circuit that implements the algorithm. This will be explained in detail in Section 3.3.

3.3 Algorithm for Approximating the Jones Polynomial in DQC1

We now have all the tools required to formulate the algorithm that will approximate the Jones polynomial at $t = e^{2i\pi/5}$. The original algorithm is the work of Ref. [SJ08], however the algorithm detailed in this section has been modified to better suit our experimental considerations. Changing the form of the Zeckendorf representation, as mentioned in the previous section, is the major modification, leading to a change in the circuit to implement the algorithm, explained below.

In Section 3.2 we described the Fibonacci basis vectors that are required to formulate this algorithm. In order to determine what size Fibonacci basis vectors we need, we look at the number of strands in our braid and place the Fibonacci basis vectors underneath the braid, with one element between every two strands, as in Figure 3.13. For an n-strand braid, this gives $m = n + 1$ elements in our basis vectors. Since we are only interested in the basis vectors that begin with an unmarked particle ($*$), we place only these vectors underneath the braid.

Using the z' Zeckendorf representation from Eqn. (3.9), the Fibonacci vectors in Fig. 3.13

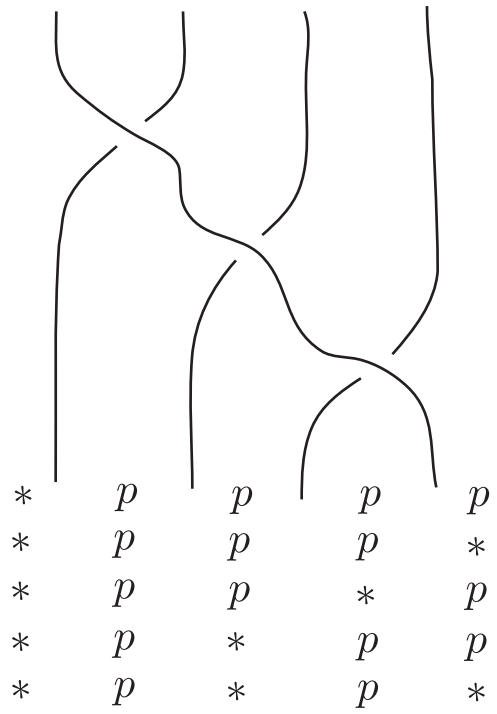

Figure 3.13: A four strand braid characterized by the elementary crossings $\sigma_1\sigma_2\sigma_3$ with the Fibonacci basis vectors that begin with the unmarked particle, $(*)$, positioned underneath and have no two unmarked particles beside each other. The four strand braid requires vectors consisting of five Fibonacci particles, and these basis vectors constitute the basis for our Jones polynomial approximation.

correspond to

$$\begin{aligned} *pppp &\rightarrow 0 \rightarrow 000 \\ *pp*p &\rightarrow 1 \rightarrow 001 \\ *p*pp &\rightarrow 2 \rightarrow 010 \\ *ppp* &\rightarrow 4 \rightarrow 100 \\ *p*p* &\rightarrow 5 \rightarrow 101. \end{aligned}$$

By converting the Fibonacci vectors to numbers via the Zeckendorf representation, and then into base 2 notation, it is clear that we require three qubits to encode these vectors. However, it is important to note that these three qubit states do not form a complete basis. The unused basis states that result from our choice of Zeckendorf representation are not a problem for the Jones polynomial approximation, as they will simply add a constant value to the trace, which can be accounted for in our final calculation.

Now that we have an understanding of the basis encoding for this algorithm, we will look at the generation of the unitary matrices required to approximate the Jones polynomial in DQC1. There is a unitary transformation corresponding to every elementary crossing in the braid. These unitaries are generated using the rules given in Eqns. (3.10)–(3.14), which are unchanged from the original algorithm in Ref. [SJ08]. The middle elements on the left hand side of the equations are marked with hats at the location of a crossing, if the vector was placed underneath the braid as it is in Figure 3.13. We can think of the braid *uncrossing* by the following rules:

$$*\hat{p}p = a(*pp) \tag{3.10}$$

$$*\hat{p}* = b(*p*) \tag{3.11}$$

$$p\hat{*}p = c(p*p) + d(ppp) \tag{3.12}$$

$$p\hat{p}* = a(pp*) \tag{3.13}$$

$$p\hat{p}p = d(p*p) + e(ppp), \tag{3.14}$$

where

$$\begin{aligned} a &= -A^4 \\ b &= A^8 \\ c &= A^8\tau^2 - A^4\tau \\ d &= A^8\tau^{3/2} + A^4\tau^{3/2} \\ e &= A^8\tau - A^4\tau^2 \\ A &= e^{-i3\pi/5} \\ \tau &= \frac{2}{1+\sqrt{5}} = \phi^{-1}, \end{aligned} \tag{3.15}$$

and ϕ is the golden ratio. For example, when generating the unitary transformation corresponding to σ_1, we look at the first three elements in the basis vectors, as these are in the position of the elementary crossing. The first three strands in each basis vector are then *uncrossed* according to the above rules, and the resulting matrix is

$$\sigma_1 = \begin{array}{c} *pppp \\ *pp*p \\ *p*pp \\ -- \\ *ppp* \\ *p*p* \\ -- \\ -- \end{array} \begin{pmatrix} a & & & & & & & \\ & a & & & & & & \\ & & b & & & & & \\ & & & 1 & & & & \\ & & & & a & & & \\ & & & & & b & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix}, \tag{3.16}$$

where the order of the basis vectors is indicated on the left hand side of the matrix and white space indicates a zero value for that matrix element. Both σ_2 and σ_3 in Eqn. (3.17) contain off-diagonal elements. The ordering of the basis vectors is consistent with their z' representation, and where there are unused basis vectors, a one has been placed along the diagonal. As mentioned previously, this additional term will be accounted for in the final approximation of the Jones polynomial. The unitary matrices corresponding to the other

two elementary crossings, σ_2 and σ_3, are

$$\sigma_2 = \begin{pmatrix} e & & d & & & & & \\ & a & & & & & & \\ d & & c & & & & & \\ & & & 1 & & & & \\ & & & & e & d & & \\ & & & & d & c & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix}, \text{ and } \sigma_3 = \begin{pmatrix} e & d & & & & & & \\ d & c & & & & & & \\ & & a & & & & & \\ & & & 1 & & & & \\ & & & & a & & & \\ & & & & & b & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{pmatrix}. \tag{3.17}$$

Note that while the rules in Eqns. (3.10)–(3.14) are unchanged from Ref. [SJ08], the unitary transformations used in this algorithm are different due to the different encoding of the basis states.

In order to approximate the Jones polynomial at $t = e^{2i\pi/5}$ using the DQC1-model we take the weighted trace of a unitary that describes the braid representation of a knot. This unitary is created by multiplying the unitaries from each elementary crossing in the braid (given in Eqns. (3.16) and (3.17)). Then the Jones polynomial at $t = e^{2i\pi/5}$ is given by

$$V(t|_{e^{i2\pi/5}}) = (-(e^{i2\pi/5})^4)^{3w}\phi^{-1}\Big(2^{n-1}(1+\phi)\mathcal{M} - \kappa\Big), \tag{3.18}$$

where w is the writhe of the braid, $\phi = (1+\sqrt{5})/2$ is the golden ratio, $\kappa = (2^{n-1} - f_m)\phi + (2^{n-1} - f_{m-1})$, n is the number of qubits in the bottom register, and $m = n + 1$ is the number of elements in the Fibonacci basis vectors. The remaining undefined parameter in Eqn. (3.18) is the trace parameter $\mathcal{M}$ is given by

$$\mathcal{M} = \frac{\mathrm{WTr}(U_n)}{2^{n-1}(1+\phi)}, \tag{3.19}$$

where WTr is the weighted trace defined by

$$\begin{aligned} \mathrm{WTr} \;=\; & 1 \;\times(\text{trace of subspace } *\ldots*) + \\ & \phi \;\times(\text{trace of subspace } *\ldots p). \end{aligned}$$

Recall that the DQC1 model of computation results in a measure of the trace of a unitary, where the top register is initially in a pseudopure state and the qubits in the

bottom register are in the maximally mixed state. We have identified a new way to directly measure the weighted trace using DQC1 by purifying the top qubit in the bottom register and rotating it in order to implement the desired weights. Recall that when discussing our Zeckendorf representation, we indicated that we wanted to separate the $*\ldots p$ and $*\ldots*$ subspaces into the subspaces where the first qubit of the bottom register was in the $|0\rangle$ and $|1\rangle$ states, respectively. Then, by rotating this state we are able to apply a different weight to the first and second half of the diagonal elements of the unitary. In our case, by purifying the first qubit in the bottom register and performing a rotation that transforms $|0\rangle$ to $(\sqrt{\phi}|0\rangle + |1\rangle)/\sqrt{1+\phi}$, we ensure that the subspace of basis vectors with $*\ldots p$ have weight $\phi/(1+\phi)$ and the subspace with basis vectors of the form $*\ldots*$ have weighting $1/(1+\phi)$. The unitary that implements this rotation is given by

$$R = \frac{1}{\sqrt{1+\phi}} \begin{pmatrix} \sqrt{\phi} & -1 \\ 1 & \sqrt{\phi} \end{pmatrix}. \tag{3.20}$$

This explains the motivation behind the form of our z'-representation, which ensures the basis states are arranged in such a way as to each receive the correct weight. This also explains the form of the κ term in Eqn. (3.18), whose sole purpose is to subtract the added value that was given to the trace by the unused basis vectors.

The computational model now contains two initialized qubits. However, this modification does not change the computational power as DQC(k) is known to have the same computational power as DQC1, provided k scales at most logarithmically with the total number of qubits [SJ08]. The circuit for our evaluation of the Jones polynomial for four-strand braids can be seen in Figure 3.14. It is worthwhile to note that the off-diagonal elements in the rotated pseudopure qubit do not contribute to the result as the unitary matrices U_n are always block diagonal, thereby eliminating the off-diagonal elements in the calculation of the trace. The state of the top qubit at the completion of the algorithm is

$$\rho_A = \frac{1}{2^{n-1}(1+\phi)} \begin{pmatrix} 1 & \mathrm{WTr}(U_n^\dagger) \\ \mathrm{WTr}(U_n) & 1 \end{pmatrix}, \tag{3.21}$$

which upon measurement of $\langle\sigma_x\rangle$ and $\langle\sigma_y\rangle$ yields the real and imaginary parts of $\mathcal{M} = \mathrm{WTr}(U_n)/(2^{n-1}(1+\phi))$ respectively, where n is the number of qubits in the bottom register. The measured quantity $\mathcal{M}$ is then used to calculate the approximation of the Jones polynomial, $V(t)$, as described in Eqn. (3.18).

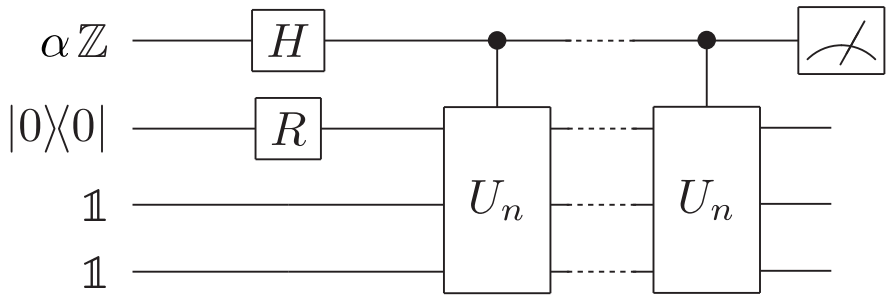

Figure 3.14: Circuit diagram for the approximation of the Jones polynomial for the knots whose braid representations consist of four strands. The number of crossings in the braid representation dictates how many controlled-unitaries are implemented. The deviation matrix for the initial state is given. The single qubit gates are the Hadamard and the rotation for implementing the weights of the trace. The measurements performed on the top qubit are expectation values of the Pauli–x and y operators.

3.4 Experimental Implementation

In this section, we detail the liquid-state NMR implementation of the algorithm described above for the set of knots whose braid representations have four strands and three crossings. There are six distinct, oriented knots in this set, which are shown in Figure 3.15, with their corresponding Jones polynomials evaluated at $t = e^{2i\pi/5}$. The goal of the experiment is to distinguish between two distinct knots given their braid representations. Note that different values for the Jones polynomial indicate topologically inequivalent knots, but identical values of the Jones polynomial do not allow us to conclude the knots are the same, since distinct polynomials may have the same value at $t = e^{2i\pi/5}$. We implement experiments for 18 different braid representations, with three different braid representations for each distinct knot, as shown in Table 3.1. All knots with the exception of knots 1 and 2 have more braid representations than were implemented.

For four strands, the Fibonacci basis vectors have five elements, and the subspaces of interest, $*\ldots p$ and $*\ldots *$ have $f_4 = 3$ and $f_{4-1} = 2$ basis states respectively. Thus, the encoding of the basis states requires 3 qubits in the bottom register and a fourth as the control qubit. Our four qubits are the four carbon-13 nuclei in crotonic acid, while the hydrogen are decoupled using the WALTZ-16 composite pulse sequence [SKF83].

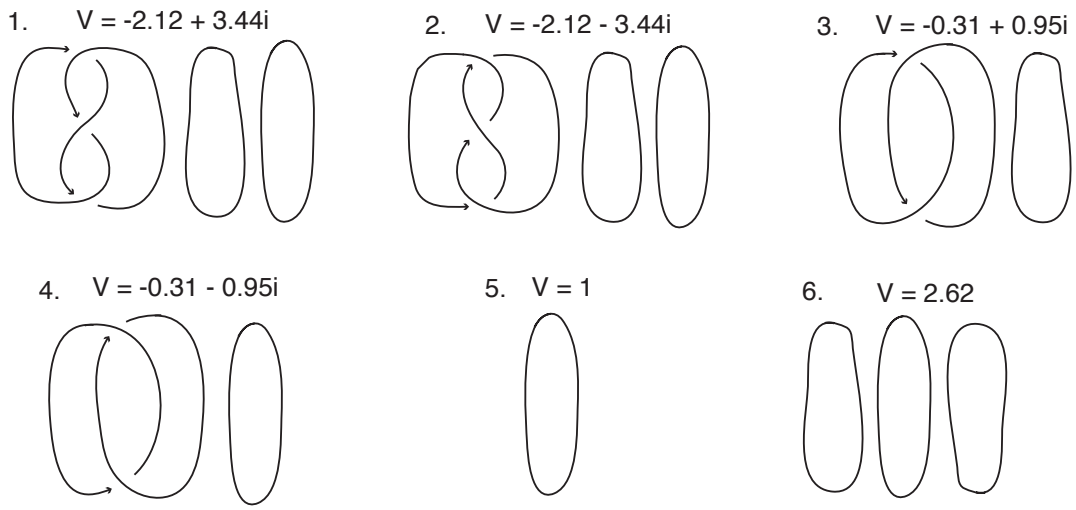

Figure 3.15: These are the six topologically distinct oriented knots whose braid representations have four strands and exactly three crossings. The values of the Jones polynomial at the point $t = e^{2i\pi/5}$ for each knot are indicated. The experimentally implemented braids corresponding to these knots can be seen in Table 3.1.

Knot 1	Knot 2	Knot 3	Knot 4	Knot 5	Knot 6
$\sigma_1^{-1}\sigma_1^{-1}\sigma_1^{-1}$	$\sigma_1\sigma_1\sigma_1$	$\sigma_1^{-1}\sigma_1^{-1}\sigma_2^{-1}$	$\sigma_1\sigma_1\sigma_2$	$\sigma_1\sigma_2\sigma_3$	$\sigma_1\sigma_1\sigma_1^{-1}$
$\sigma_2^{-1}\sigma_2^{-1}\sigma_2^{-1}$	$\sigma_2\sigma_2\sigma_2$	$\sigma_2^{-1}\sigma_2^{-1}\sigma_1$	$\sigma_2\sigma_2\sigma_3^{-1}$	$\sigma_2\sigma_3\sigma_1^{-1}$	$\sigma_2\sigma_2\sigma_2^{-1}$
$\sigma_3^{-1}\sigma_3^{-1}\sigma_3^{-1}$	$\sigma_3\sigma_3\sigma_3$	$\sigma_3^{-1}\sigma_3^{-1}\sigma_2$	$\sigma_3\sigma_3\sigma_1^{-1}$	$\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}$	$\sigma_3\sigma_3\sigma_3^{-1}$

Table 3.1: The experimentally implemented braids and their corresponding knots. The knots and the approximation of their Jones polynomials at $e^{2i\pi/5}$ are given in Figure 3.15. Note that there are more braids that yield knots $3-6$ than those listed above.

Information about the molecule as well as a detailed description of the experimental setup is found in Appendix A. C_1 is our readout qubit, whose initial state is given by the deviation density matrix $\rho_{C1} = Z$, C_2 is purified to the pseudopure state $|0\rangle\langle 0|$, and the remaining C_3 and C_4 are initialized to the completely mixed state. Pulses for the controlled unitary operations, given in Eqns. (3.16) and (3.17), their inverses, the rotation and Hadamard gates were numerically optimized to have fidelities of 0.998 using the GRAPE algorithm (see Section 2.1.2) and to be robust against small ($\pm 3\%$) inhomogeneities in the r.f. field. The controlled unitaries are each 60ms in length while the single qubit gates are 600μs. The pulses are corrected for nonlinearities in the pulse generation and transmission to the sample by measuring the r.f. signal at the position of the sample using a feedback loop and iteratively modifying the pulse accordingly. Through the feedback loop, the implemented pulse was found to have a simulated fidelity of 0.99 after correction. More information about this procedure can be found in the doctoral dissertation of Dr. Colm Ryan [Rya08] and in Appendix A.

At the end of the algorithm, the fitted spectrum of C_1 is compared to a reference spectrum. Traditionally, the reference spectrum is of the initial state – however, due to the complex nature and length of this experiment, comparing the final result to the initial state was not sufficient. Figure 3.16 shows the difference in signal strength after the pseudopure state creation and the end of a reference experiment where pulses whose propagator was designed to be the identity were generated using GRAPE to have the same length and the same average power and fidelity as the controlled-σ_i were implemented. In the absence of decoherence effects and other errors, we would expect these two spectra to be identical. In an attempt to normalize some decoherence effects, we used the state at the end of the reference experiment to compare to the final state. This is a crucial step in the experimental

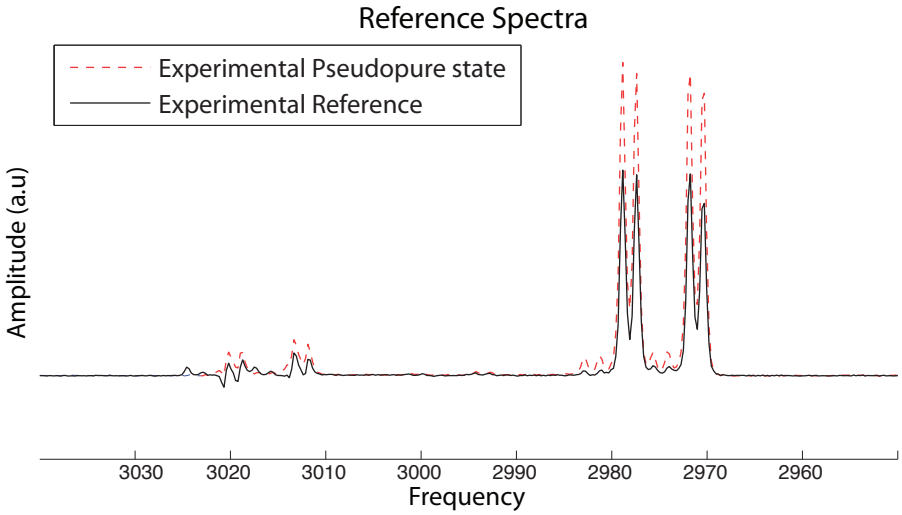

Figure 3.16: Spectra of the initial state of C_1 both with and without reference identity pulses. The dotted red line shows the state immediately after preparing the pseudopure state and the solid black line shows the pseudopure state after three successive 60 ms pulses designed to implement the identity. These pulses were generated using GRAPE to have the same average power and length of the controlled unitary pulses used in the experiment. The state after these reference identity pulses was chosen to act as the reference for the experiment in an attempt to normalize some of the decoherence effects.

procedure, as the state measured after three successive identity pulses, totalling 180 ms had only 60% of the original signal (see Figure 3.16). This is not surprising, given that the T_2 for the carbon nuclei is approximately 1s, indicating that the length of the controlled-unitaries is $0.18T_2$. Pulses of this length were required due to the complicated nature of the pulses: they required coupling between all four qubits.

Another difficulty experienced in this experiment was the need to decouple the hydrogen nuclei throughout the experiment. The decoupling procedure is not perfect, and because we are decoupling more than one proton, off-resonant effects arise. We found that very small changes in the decoupling parameters (length between pulses, frequency, and power) had a large impact on the carbon spectrum. In order to better decouple certain spins, we sacrificed others. In addition to these errors, decoupling procedures require con-

stant pulsing, which heats the sample and changes the Hamiltonian slightly. For future experiments, my recommendation would be to avoid decoupling for long experiments or those that require extreme precision. This can be done by using a different molecule or preparing the unused spins in a pseudopure state.

Finally, in addition to implementation difficulties, we found subtle problems with the pulse generation methods used. When using the GRAPE algorithm to numerically generate the pulses, we use the fitness function of the gate fidelity $F_g(U_{sim}, U_{goal}) = |\mathrm{Tr}(U_{goal}^{\dagger} U_{sim})|^2/d^2$ to determine how faithful the generated pulse is to the ideal pulse. However, in a DQC1 algorithm we are making a very specific measurement: one resulting in the trace of the unitary. One can imagine that while a given unitary may have a gate fidelity of 0.998, it may have errors concentrated along the diagonal. The consequences of this idea are fleshed out in Appendix A.1 where we found that indeed, it is likely to effect our experiment. In order to get around this problem, in addition to creating a pulse with high gate fidelity, we ensured it had a "well-behaved" trace. This two-part pulsefinding procedure is not ideal, and a solution to this problem is of great interest.

3.5 Results

In this section, we report the results of the experiment to approximate the Jones polynomial at $t = e^{2i\pi/5}$ using DQC1. The results are found by fitting the spectra at the conclusion of the DQC1 algorithm, which allows us to measure the trace. The output spectrum of C1 for the experiment implementing the unitary corresponding to the braid $\sigma_1\sigma_2\sigma_3$ is shown in Figure 3.17 together with the simulated spectra. The fitted spectra are then integrated to find the real and imaginary components of the weighted trace, whose definition is given in Eqn. (3.19). This procedure is followed for 18 different braid representations and the value of the Jones polynomial, approximated at $t = e^{2i\pi/5}$, is displayed in Figure 3.18 for all 18 experiments.

Systematic errors from imperfect initial state preparation and decoherence not captured by the reference state result in the offsets from the theoretical values. The main contribution to the spreading of the experimental points is the finite fidelity of the pulses. As mentioned in the previous section, we have measured the pulse at the sample and found that it has a simulated fidelity of 0.99. We then simulated the experiment performed with 0.99 fidelity to find the statistical error present. The error ellipses given in Figure 3.18

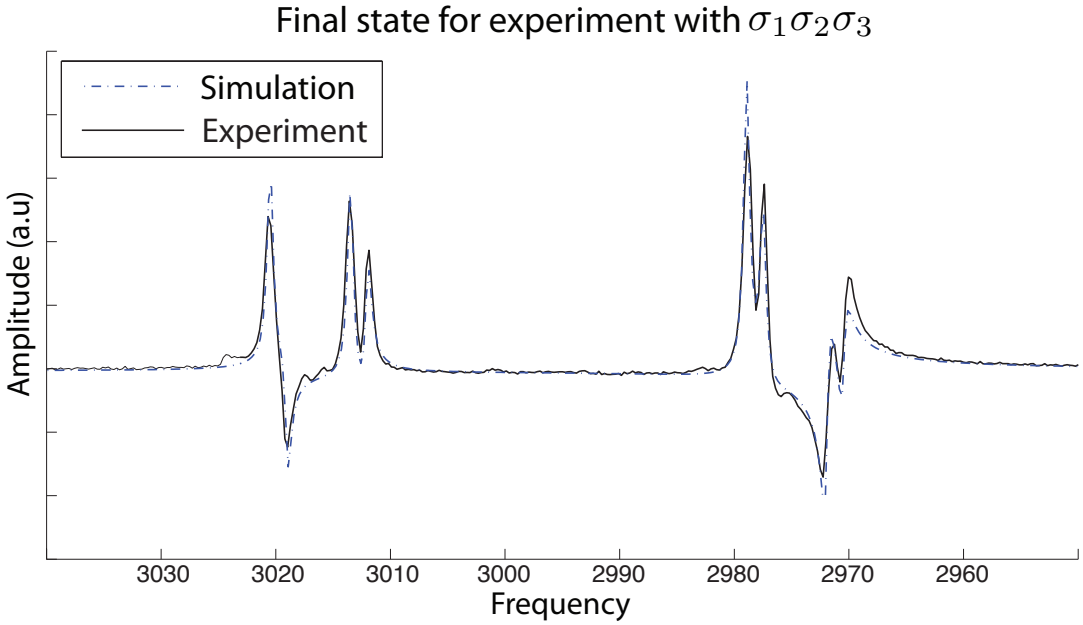

Figure 3.17: Spectra of the final state of an instance of the experiment to approximate the Jones polynomial using a DQC1 algorithm. The spectrum shown here is of C_1 after the unitary transformations associated with a four-strand braid with elementary crossings corresponding to $\sigma_1\sigma_2\sigma_3$, a braid representation of knot 5. The solid black line shows the experimental data and the blue dashed line is the scaled simulation, highlighting the level of control in our experiment. The real part of the weighted trace is proportional to the integral of this spectrum. The imaginary part of the weighted trace is proportional to the integral of the spectrum phased by 90 degrees.

demonstrate the statistical error with 86.5% confidence levels or 2 standard deviations. These error ellipses are used to determine if two knots are distinct.

Two values of the Jones polynomial at best can distinguish between two knots if they are sufficiently far apart, and at worst, give no information, as even evaluations of the Jones polynomial that are identical would not be sufficient information to conclude that the two knots are identical. This leads to two types of errors when interpreting the data: *passive* and *fatal* errors. Passive errors occur when two distinct knots are impossible to distinguish because of their relatively close distance to one another, while fatal errors occur when two identical knots are determined to be distinct. The success rate for determining whether knots are distinct is calculated as the average of the percent of distinct knots correctly identified and the percent of identical knots correctly indistinguishable:

$$\text{success rate} = \frac{1}{2}\left(\frac{\text{passive errors}}{\text{pairs of distinct knots}} + \frac{\text{fatal errors}}{\text{pairs of identical knots}}\right). \tag{3.22}$$

The error ellipses give a direct method for determining if two knots are distinct. If the error ellipses for a pair of knots do not overlap then it is inferred that the knots are distinct; if the two ellipses overlap no information is gained. For the confidence region plotted in Figure 3.18, 134 of the possible 135 pairs of distinct knots are correctly distinguished with 3 fatal errors of a possible 18, corresponding to a success rate of 91%. Note that the reason the error ellipses in Figure 3.18 do not overlap with the theoretical values is because we did not analyze all sources of error in the experiment. Because our goal was simply to distinguish distinct knots, further analysis of the experimental errors was not necessary.

3.6 Conclusion

In this chapter, we experimentally implemented an instance of the DQC1 model of computation to approximate the Jones polynomial for a set of knots whose braid representations have four strands and exactly three crossings. This experiment was chosen for several reasons. One of these is that approximation of the Jones polynomial is a problem with no known efficient classical algorithm and has applications in a wide range of fields. In addition, it is a complete problem for the DQC1 model of mixed state computation, which has very little entanglement yet provides an advantage over classical methods. Finally, the experiment requires extremely good control over a long period of time, and therefore, is a

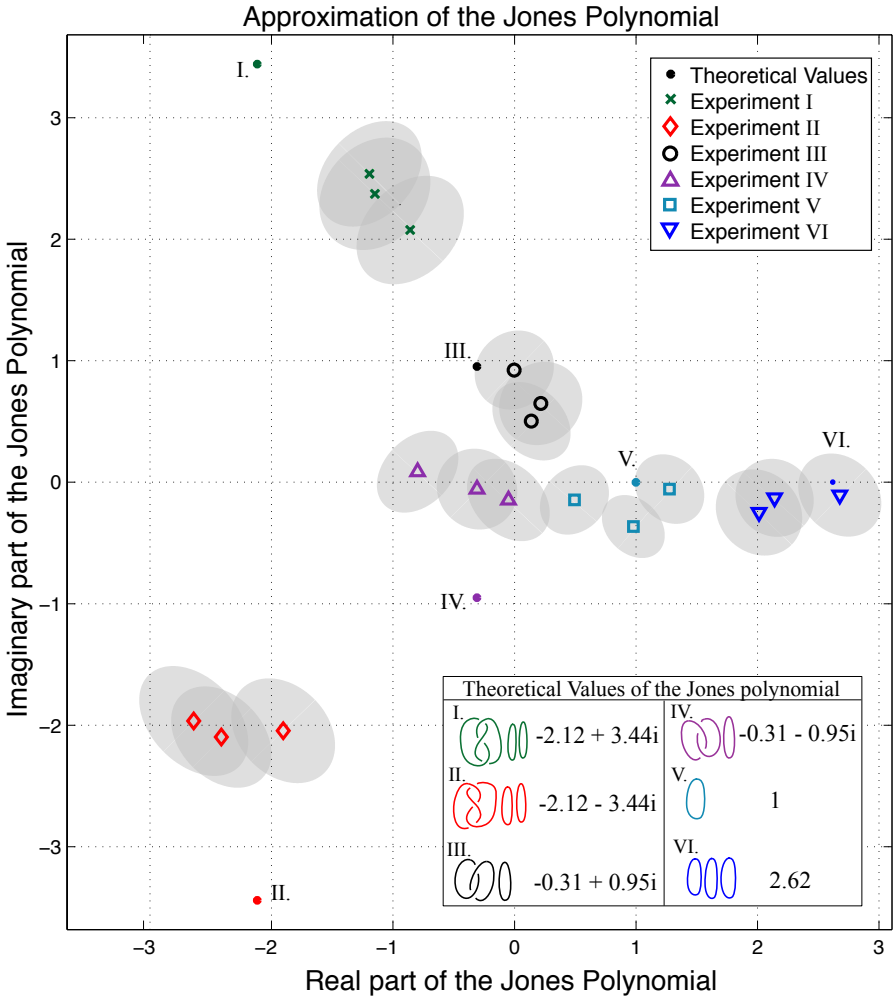

Figure 3.18: The results for the approximation of the Jones polynomial for knots whose braid representations have four strands and three crossings. There are six unique knots of this kind and their theoretical values of the Jones polynomial at the point $t = e^{2i\pi/5}$ are plotted for each of the six experiments. The corresponding experimental data points of three braid representations for each experiment are plotted, along with error ellipses demonstrating the statistical error (with 86.5% confidence levels or 2σ). The distribution is generated by simulating each experiment 200 times with single pulse fidelities of 0.99 which is the implemented pulse fidelity. Using the error ellipses as discriminators, these results yields a 91% success rate for distinguishing distinct knots, calculated using Eqn. (3.22).

good test for how well current NMR quantum information processors can solve quantitative DQC1 problems.

This experimental implementation was based on an algorithm developed in Ref. [SJ08], that was modified to suit the needs of our particular experiment. Our modification was motivated by finding a unique way to measure the weighted trace of a unitary. In order to perform the weighted trace by using an additional pure qubit, we had to modify the encoding of the basis vectors. This is done by creating a different Zeckendorf representation than that used in the original algorithm. This changed the problem to a DQC(2) computation, which only adds a constant overhead, and is as powerful as DQC1 as the number of maximally mixed qubits grow [SJ08].

Our experiment was performed on four qubits in liquid state NMR. Within the set of knots whose braid representations have three crossings over four strands, we were 91% successful at distinguishing distinct knots. These results show the extremely precise implementation of a difficult quantum algorithm, pushing the boundaries of control in NMR. In future work, it would be interesting to see how the values of the Jones polynomial spread as you increase the number of strands and crossings in the braid representations, in order to determine what size knot can be experimentally examined before noise and control errors destroy the quantum advantage.

Chapter 4

Experimentally detecting non-classical correlations in a mixed-state computation

In previous chapters we have explained the computational model of DQC1 and used it to experimentally approximate the Jones polynomial, an important problem that cannot be efficiently solved by today's classical methods. We have also briefly discussed the correlations present in the mixed states of the DQC1 model, indicating that they contain very little, or no, entanglement. However, even in the bipartite splitting that gives rise to zero entanglement, it can contain nonclassical correlations as measured by the quantum discord [DSC08]. Quantum discord, as explained in Section 2.2.2, is a measure of the correlations that exist in excess of those present in classical states. It is measured by the difference in two classically equivalent formulations of the mutual information, where a non-zero value indicates a deviation from purely classical correlations [HV01, OZ01]. It is not yet known whether or not quantum discord assists quantum algorithms, but it is a good candidate for the computational advantage offered by the DQC1 model, and understanding it better will certainly provide insights into the workings of quantum systems and algorithms.

While it has been shown that almost every quantum state has quantum discord [FAC$^+$10], Datta, Shaji, and Caves showed that, on average, the quantum discord present in a DQC1 algorithm drops with a decrease in polarization [DSC08]. Typical liquid-state nuclear

magnetic resonance (NMR) experiments are performed at room temperature, and the unentangled initial states have very small polarization. Therefore, the following question remains: is it possible to experimentally detect quantum discord in a DQC1 algorithm where the polarization is very small?

In this chapter we report on the experimental detection of non-classical correlations in the output state of a DQC1 algorithm in NMR, using a state-independent non-zero discord witness. Similar to entanglement, calculation of the quantum discord for a general state requires full tomographic data; therefore, witnesses that detect the existence of these correlations are a practical alternative. This experiment is the first physical implementation of a non-linear discord witness that can detect discord in any state of any size. We are able to detect discord without full tomographic data, using instead only a few experiments for a four-qubit system.

The results of this work have been published in Physical Review A [PMTL11], copyright (2011) by the American Physical Society. The experiment was performed by the author of this thesis, who benefited from the assistance of O. Moussa during the planning stages and throughout data analysis and interpretation. D. A. Trottier assisted on this project for several months, working with the computational analysis.

This chapter proceeds as follows: Section 4.1 explains how quantum discord witnesses work and summarizes several different witnesses from the literature. The experimental setup is detailed in Section 4.2, and the results are given in Section 4.3. The chapter concludes with a discussion of the results.

4.1 Witnessing Quantum Discord

In order to calculate the quantum discord in a particular state, full knowledge of the quantum state and a minimization over all projective measurements is required. Quantum state tomography is very expensive, as the number of resources required grows exponentially with the number of qubits in the system – making it very impractical. Measuring the entanglement in a system suffers from the same requirement. As a result of this requirement, soon after entanglement measures were articulated, entanglement witnesses were created [HHH96, Ter00], the basics of which can be read in Section 2.2.1. Discord witnesses have been created with exactly the same idea. In this section we discuss discord witnesses and describe the witness used in our experimental work.

4.1.1 States with zero quantum discord

Before defining a discord witness, it is important to take a better look at states that have zero discord. Zero discord states were categorized in Section 2.2.2 as CQ states with $D(A:B) = 0$, QC states with $D(B:A) = 0$ and CC states where $D(A:B) = D(B:A) = 0$. In this chapter we are going to be concentrating on CQ states. A necessary and sufficient condition for a bipartite quantum state having zero discord $D(A:B)$ is that there exists a measurement $\{\Pi_k\}$ such that

$$\rho_{AB} = \sum_k (\Pi_k \otimes I)\rho_{AB}(\Pi_k \otimes I), \tag{4.1}$$

where $\{\Pi_k\}$ is a projective measurement acting on subsystem A [Dat08]. A similar expression exists for states with zero discord $D(B:A)$, where the measurement is performed on subsystem B. The above statement appears very intuitive: if a measurement on system A does not disturb or affect the total state, then the system contains no correlations in excess of those that exist in classical systems. This is in agreement with our definition of classical and quantum correlations given in Section 2.2, where we defined classical correlations as those that can be locally accessed without disturbing the total system.

Alternatively, we can say that the state ρ_{AB} has zero quantum discord when it is block diagonal in the eigenbasis of the reduced (marginal) state of system A. This criteria can be seen by directly looking at the definition for CQ states (states with zero discord $D(A:B)$): $\rho_{AB} = \sum_j p_j |j\rangle\langle j| \otimes \rho_j^B$, where $\{|j\rangle\}$ is an eigenbasis for ρ_A.

Looking at the state originally given in Eqn. (2.51),

$$\rho_{AB} = \frac{1}{2}(|0\rangle\langle 0| \otimes |-\rangle\langle -| \; + \; |1\rangle\langle 1| \otimes |0\rangle\langle 0|),$$

we can demonstrate these two criteria for states with zero discord. For this simple example, it is straightforward to see that there exists a measurement on system A (in this case, in the computational basis), that does not effect the state, indicating that there is zero discord, $D(A:B)$. On the other hand, we can see that there is no such measurement on system B that does not disturb the state of the system. Equivalently, we could have written this state in its matrix form:

$$\rho_{AB} = \frac{1}{2}\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

In this example, the marginal eigenbasis of ρ_A is the computational basis, and when we write the density matrix in that basis, it is easy to see that it is block diagonal. Another state whose marginal eigenbasis is the computational basis is the Werner state given in Eqn. (2.55):

$$\begin{aligned}\rho_W &= \frac{(1-z)}{4} I^{\otimes 2} + z|\psi_+\rangle\langle\psi_+| \\ &= \frac{1}{4}\begin{pmatrix} 1+z & 0 & 0 & 2z \\ 0 & 1-z & 0 & 0 \\ 0 & 0 & 1-z & 0 \\ 2z & 0 & 0 & 1+z \end{pmatrix},\end{aligned}$$

which is not block diagonal for any value $z \neq 0$. This is consistent with what we found in Section 2.2.2: ρ_W has non-zero quantum discord for any non-zero value of z. For more information on criteria for vanishing quantum discord, please see Refs. [HWZ11] and [Dat10].

Zero discord states in NMR

Typical NMR experiments have very small polarization, which lead to very small amounts of quantum discord. One of the difficulties in measuring discord or similar properties in an NMR experiment is that we only measure the pseudopure state in traditional experiments. Recall that NMR states can be written as a mixture of the identity and a pseudopure state,

$$\rho_{NMR} = \frac{1-\alpha}{2^n} I + \alpha \rho_{pps}.$$

Experimentally, pseudopure states are measured and compared to a known state that serves as a reference for α. If we detect the presence of quantum discord in the pseudopure state, a priori, it is not known whether or not the physical state contains discord. However, it turns out that detecting discord in the pseudopure state is sufficient for detecting discord in the physical state (ρ_{NMR}). The proof of this statement is shown below.

Recall that a necessary and sufficient condition for a state ρ to have zero discord is that there exist a projective measure $\{\Pi_k\}$ such that

$$\rho = \sum_k (\Pi_k \otimes \mathbb{I})\rho(\Pi_k \otimes \mathbb{I}). \tag{4.2}$$

Analyzing this condition for ρ_{NMR}:

$$\begin{aligned}
\sum_k (\Pi_k \otimes \mathbb{I}) \rho_{NMR} (\Pi_k \otimes \mathbb{I}) &= \rho_{NMR} \\
\sum_k (\Pi_k \otimes \mathbb{I}) \left(\frac{(1-\alpha)}{2^n} \mathbb{I} + \alpha \rho_{pps} \right) (\Pi_k \otimes \mathbb{I}) &= \frac{(1-\alpha)}{2^n} \mathbb{I} + \alpha \rho_{pps} \\
\Rightarrow \frac{(1-\alpha)}{2^n} \mathbb{I} + \sum_k (\Pi_k \otimes \mathbb{I}) \alpha \rho_{pps} (\Pi_k \otimes \mathbb{I}) &= \frac{(1-\alpha)}{2^n} \mathbb{I} + \alpha \rho_{pps} \\
\Rightarrow \sum_k (\Pi_k \otimes \mathbb{I}) \alpha \rho_{pps} (\Pi_k \otimes \mathbb{I}) &= \alpha \rho_{pps} \\
\Rightarrow \sum_k (\Pi_k \otimes \mathbb{I}) \rho_{pps} (\Pi_k \otimes \mathbb{I}) &= \rho_{pps}
\end{aligned}$$

for $\alpha \neq 0$. The necessary and sufficient condition for non-zero discord in the physical NMR state ρ_{NMR} is equivalent to the necessary and sufficient condition for non-zero discord in the pseudopure state ρ_{pps}. In other words, if discord is found in the pseudopure state, it indicates the presence of discord in the physical state, regardless of the amount of polarization α.

This result has also been shown in the work of A. Ferraro *et al.*[FAC+10]. They indicate that all states belonging to the set of zero discord states are connected to the maximally mixed state, and that as one rectilinearly moves any state to the maximally mixed state (this is equivalent to moving through the depolarizing channel), if the original state had zero discord, then all states towards the maximally mixed will have zero discord. If it has non-zero discord, on the other hand, then all states encountered prior to reaching the maximally mixed state will also have non-zero discord. This is in stark contrast to the existence of entanglement, which vanishes for a particular value of the polarization. Indeed, this indicates that states in the highly mixed NMR architecture can contain correlations above and beyond what is found in classical systems, as measured by the quantum discord.

4.1.2 Discord Witnesses

As mentioned above, discord witnesses are desirable due to the difficulty in measuring the amount of discord present in an experimental state. To date there have been several proposals for witnessing quantum discord, most of which are able to detect discord in a

small set of cases. Note that unlike entanglement witnesses, a discord witness is necessarily nonlinear as the set of zero discord states is not convex. Let us briefly mention them here before explaining the witness chosen for our experiment.

- A witness for the correlations shared by a system and its environment was created by Laine, Pillo and Breuer [LPB10]. This witness does not require any knowledge of the structure of the state or the initial conditions of the environment. It has been experimentally implemented in optics [SBC$^+$11].

- The discovery that $2 \times N$-dimensional states that are not strong positive partial transpose must contain non-classical correlations as measured by the quantum discord [BC10] lead to a natural witness for these states that is analogous to the Peres–Horodecki positive partial transpose (PPT) criterion for entanglement.

- A single-experiment detectable witness for use in ensemble systems was developed by Rahimi and SaiToh [RS10]. This witness requires a parameter to be determined numerically before the witness can be experimentally helpful. This witness detects CC states that have $D(A:B) = D(B:A) = 0$.

- An observable witness that works for any unknown quantum state was developed by Yu et al. [YZCO11]. It requires four copies of the state to be processed simultaneously.

- A non-linear witness for certain two-qubit states has been proposed [MS10]. The witness detects non-classical correlation if a two-qubit state written as

$$\rho = \frac{1}{4}\left(I_2 + \sum_i \left(a_i\sigma_i \otimes I + b_i I \otimes \sigma_i + c_i\sigma_i \otimes \sigma_i\right)\right)$$

  is not CC. This witness has been used to experimentally detect quantum discord in a two-qubit NMR system [AMC$^+$11]. They looked for discord in two Bell-diagonal states, one of which was a QC state and the other was CC, as well as the thermal NMR state. Recently, this witness was extended for use in arbitrary dimension [MCC11].

Finally, the witness we use in this experimental test for discord was introduced by Dakic, Vedral and Brukner in 2010 [DVB10]. They used the definition for zero discord states given in Eqn. (4.2) and proved that for a bipartite state written as

$$\rho = \sum_{n,m} r_{nm} A_n \otimes B_m, \tag{4.3}$$

where $\{A_n\}$, $\{B_m\}$ are bases of Hermitian operators, a sufficient condition for non-zero quantum discord $D(A:B)$ is that if the *correlation matrix* R with matrix elements r_{nm} has a rank greater than the dimension of system A. Similarly, for non-zero discord $D(B:A)$, the rank of the correlation matrix must be greater than the dimension of system B. Therefore, in order to witness discord in a quantum system, instead of performing exponentially many experiments to obtain the full quantum state, one only has to measure enough elements of the correlation matrix to find a rank greater than $\dim(A)$. In addition to being experimentally friendly, this witness works for states of any dimension and bipartite splitting. Details on how we measure this experimentally are given in the following section.

4.2 Experimental Detection of Quantum Discord

Using the discord witness described above, we set out to detect quantum discord in an NMR implementation of a DQC1 algorithm. While previous studies have theoretically [DSC08] and experimentally [LBAW08] shown that DQC1 contains non-classical correlations, these studies rely on full knowledge of the quantum state. This chapter details our experiment to detect quantum discord using only a small number of experiments.

Our NMR experiment is implemented using four carbon-13 labeled nuclei in crotonic acid (whose chemical structure and the Hamiltonian are found in Appendix A, along with a diagram in Figure A.1), in the liquid state. The qubits are encoded in the spin states of the spin-1/2 nuclei. The ground state bias, known as the polarization, is very small in this experiment, with a value of 1.43×10^{-5}. For this polarization and perfect implementation of the unitary transformations on the three qubits in the bottom register, the numerically computed quantum discord present at the completion of the algorithm described below, is 5.4×10^{-11}. This corresponds very well with the analytical results [DSC08] for the average discord after a DQC1 circuit for a unitary drawn uniformly by the Haar measure of approximately 7.1×10^{-11}. In this experiment we test whether or not it is possible to detect an amount of discord this small.

We tested for quantum discord at the initial and final state of the DQC1 model. The circuit diagram for each experiment can be seen in Figure 4.1. The unitary we chose is of the form $U = \mathrm{diag}(a, a, b, 1, a, b, 1, 1)$, where $a = -(e^{-i3\pi/5})^4$ and $b = (e^{-i3\pi/5})^8$, and is an important transformation in the approximation the Jones polynomial for a class of knots whose braid representations have four strands. The Jones polynomial is an important

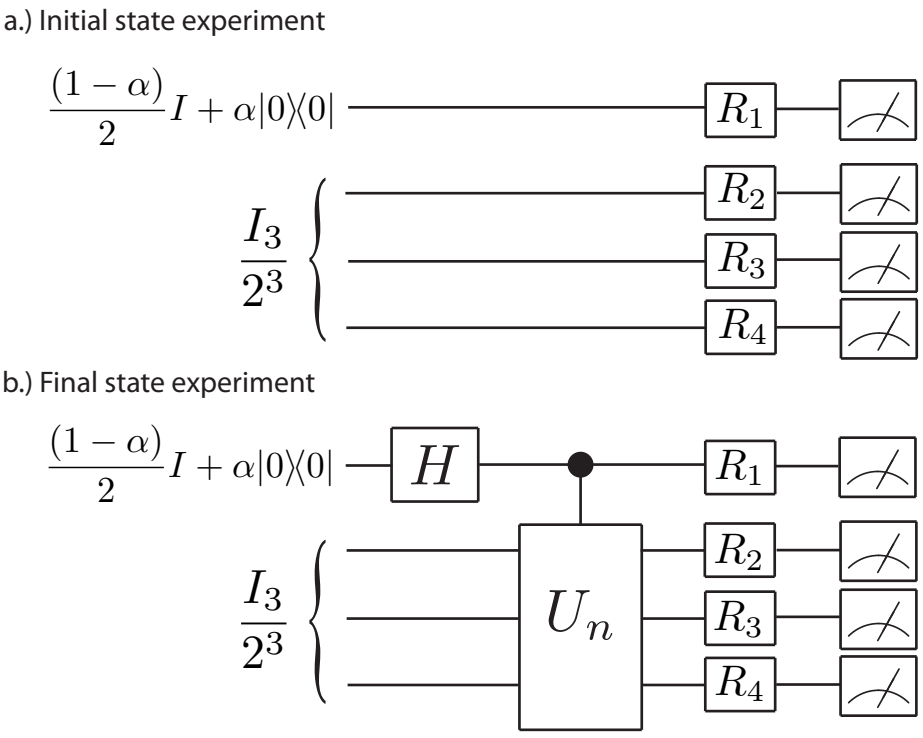

Figure 4.1: DQC1 circuit diagram to test for quantum discord in the (a) initial and (b) final states in a DQC1 experiment. The measurements are accompanied by single qubit rotations that determine the operators observed in each experiment.

application of the DQC1 model of computation as discussed in Chapter 3. For particular information regarding the NMR experimental procedure, please consult Appendix A.

We are looking to detect discord across the zero-entanglement bipartite splitting of the top and bottom register, so system A consists of a single qubit and system B of three qubits. In order to write the state in the form of Eqn. (4.3), we chose the bases of Hermitian operators to be $\{A_n\} = \{I, X, Y, Z\}$ and $\{B_m\} = \{III, IIX, IIY, IIZ, IXI, IXX, \ldots\}$, where $X = \sigma_x$ (similarly for Y and Z) and $\{B_m\}$ are all possible combinations of three qubit Pauli operators. Then, for example, the $(2, 2)$ element of the correlation matrix is, $r_{22} = \mathrm{Tr}(XIIX\rho)$. The choice of operators was made due to the ease of measuring Pauli operators in NMR. The size of our correlation matrix R is 4×64, and therefore has a maximum rank of four. In order to witness discord $D(A:B)$, we must show that the $\mathrm{rank}(R) > \dim(A) = 2$.

We determine the rank of the correlation matrix by computing the number of non-zero singular values. Finding a lower bound on the rank of a matrix does not require that all elements of the matrix be measured, only a rectangular subset. We call this rectangular subset our truncated correlations matrix, R_{trunc}, which does not have a pre-set dimension and can change size throughout the procedure. The procedure for determining if the rank is greater than two is as follows:

1. Start by measuring a subset of the correlation matrix, denoting it R_{trunc}. We chose to start with 4×4 section of the correlation matrix.

2. Determine the rank by performing a Monte Carlo sampling to determine which singular values can be reliably distinguished from zero (this procedure is explained in more detail below)

3. Proceed as follows:

   (a) If $\mathrm{rank}(R_{trunc}) > 2$: Quantum discord is detected!

   (b) If $\mathrm{rank}(R_{trunc}) \leq 2$: Since the rank is less than or equal to two, there must be linearly dependent columns in the correlation matrix. Remove any linearly dependent columns and replace by measuring an additional column of the correlation matrix. Then, repeat from step 2.

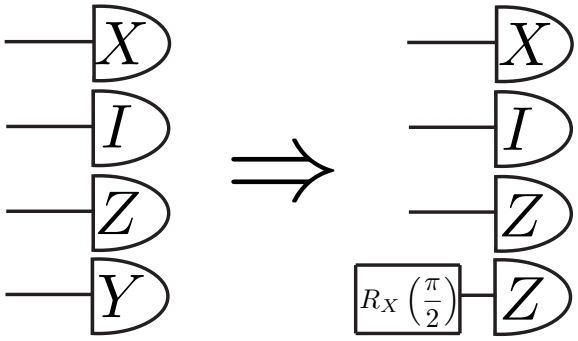

Figure 4.2: The operator $XIZY$ is not inherently observable in NMR, so in order to observe it we perform a $\pi/2$-rotation about the x-axis on the fourth qubit and observe $XIZZ$.

This procedure will continue until either quantum discord is witnessed, or the entire correlation matrix has been measured, giving full tomographic data. It is important to note here that if the rank is found to be less than the dimension of system A, we cannot conclude that the system has zero discord – our test was simply inconclusive, as $\text{rank}(R) > \dim(A)$ is sufficient but not necessary for non-zero discord.

Each experiment involved performing a readout pulse immediately before the measurement that allowed us to measure the coefficients of different operators. In NMR, the 2^n observables we measure for n qubits are X and Y on a single observed qubit, with $Z^{\otimes m} I^{\otimes n-m-1}$ and their permutations for $m = 0 \ldots n-1$. In this four-qubit experiment there are 16 observables. In order to measure each of the operators in the correlation matrix R, we perform a rotation that allows us to measure the coefficient of an operator that is not inherently observable in NMR. For instance, if you wanted to measure to operator $XIZY$ on four qubits, you could perform a readout pulse on the fourth qubit that consists of a rotation of $\pi/2$ about the x-axis, then measure the observable $XIZZ$. This can be seen graphically in Figure 4.2. An example of the spectra for the top qubit after a readout pulse of $\pi/2$-rotations about $XIYY$ and the corresponding fit are shown in Figure 4.3. More information about measuring operators in NMR can be found in Ref. [LM04].

The Monte Carlo sampling used during step 2 is required because any experimental data will always have full rank due to small errors. In order to determine the rank of our matrix that is robust against these small errors we perform a Monte Carlo sampling

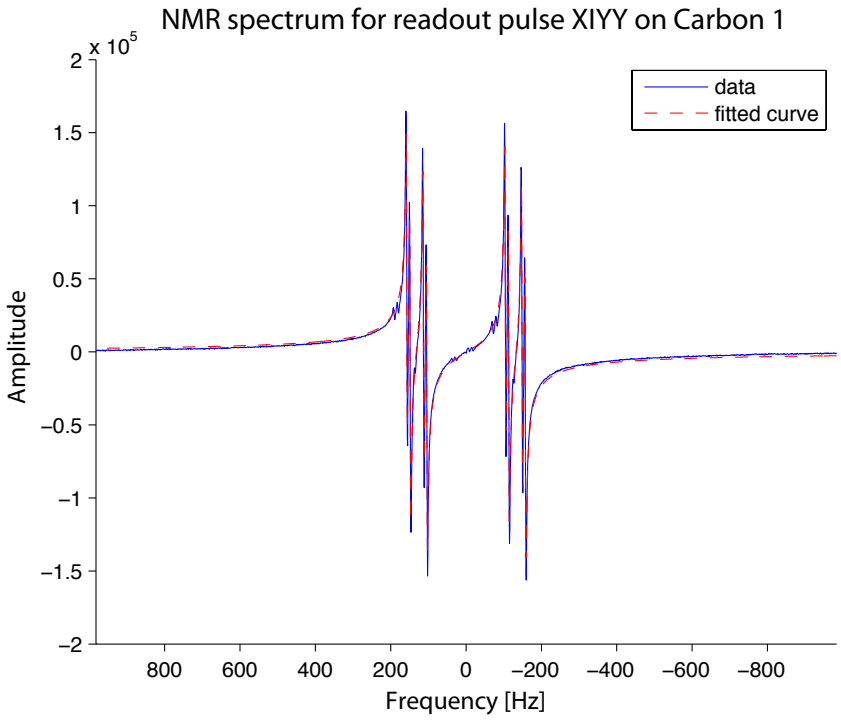

Figure 4.3: Above is the spectra resulting from the DQC1 experiment followed by a read-out pulse of XIYY. After performing the readout pulse, we are able to measure the coefficients of the following operators: $\{XIII, XIIX, XIXI,\ XIXX, XZII, XZIX,\ XZXI, XZXX,$ $ZIII, ZIIX, ZIXI,\ ZIXX, ZZII, ZZIX,\ ZZXI, ZZXX\}$. The first eight operators are measured by fitting the resulting spectrum, with the last eight operators found by fitting the spectrum above, phased by 90 degrees. This figure displays the experimental data and the fitted curve.

of each of the elements of the matrix. Each sampled element is determined by a normal distribution around the measured value, whose variance is determined by the errors in the spectral fitting process. Once a sampled value for each element is found, one set of singular values are computed. We repeat this process many times to produce a histogram of singular values (as can be seen in results Figures 4.4 and 4.5). The rank is then determined by the number of distributions that do not overlap with zero.

4.3 Experimental Results

In this section we outline the experimental results to detect discord in the initial state and the final state of the DQC1 algorithm.

4.3.1 Initial state

In measuring the correlation matrix for the initial state, we began this procedure with a 4×4 truncated matrix R_{trunc}, found a rank of 1, measured another column of the correlation matrix, found a rank of 1, and continued this process until the entire correlation matrix had been measured. Therefore, we were not able to detect any quantum discord in the initial state of the DQC1 algorithm. This result is not surprising, as simulations show zero discord in this state.

The Monte Carlo sampling only ever looked at a 4×4 truncated matrix, because we found that as the size of the matrix grew, the errors compounded, leading to much wider spreads in the histogram of singular values. Instead, we would remove one linearly dependent column as we added an additional one (item 3(b) in the procedure listed above). This ensured we were not "missing" any non-zero singular values due to a very wide spread in the histogram.

The histogram in Figure 4.4 was created using 1000 different 4×4 truncated correlation matrices, each of these R_{trunc} was sampled 10 times. Every truncated correlation matrix R_{trunc} was composed of the first column (which includes the $IIII$ component, which is known to be exactly 1) and three other random chosen columns. As can be seen, there is one singular value around 1.4, due to the $IIII$ element, and three others centred around zero. The cumulative function is included in the figure to assist the reader in determining

the integral of the distribution, which indicates the number of singular values accounted for.

4.3.2 Final state

When measuring the final state, we began by measuring columns corresponding to $B_m = \{III, IZI, IIZ, IZZ\}$. Recall that the rows correspond to $A_n = \{I, X, Y, Z\}$. The experimentally measured truncated correlation matrix is

$$R_{trunc} = \begin{pmatrix} 1 & -0.01 & 0.00 & -0.01 \\ 0.10 & -0.34 & -0.13 & 0.25 \\ 0.17 & 0.38 & 0.04 & 0.26 \\ 0.01 & 0.08 & -0.01 & 0.02 \end{pmatrix} \pm \begin{pmatrix} 0 & 0.007 & 0.01 & 0.007 \\ 0.05 & 0.05 & 0.05 & 0.05 \\ 0.05 & 0.05 & 0.05 & 0.05 \\ 0.04 & 0.007 & 0.007 & 0.007 \end{pmatrix}, \tag{4.4}$$

where the errors reported are propagated through linear inversion from spectral peak-fitting, and correspond to a 68.2% confidence level in the results of the fitting process. Each matrix element is calculated using linear inversion of variables fitted directly from the NMR spectrum. In order to obtain these results, four instances of the experiment were required, each with a different readout pulse and observing a different spin. Note that the matrix element corresponding to the operator $IIII$ has no error associated with it, which is because this term is not measured, but is known to be one in order to ensure that trace$(\rho) = 1$. All values in the correlation matrix are measured as a fraction of the polarization α by comparing with a reference state.

Without performing any further data analysis, it is possible to estimate that the correlation matrix of the final state has a rank of at least three, by simply inspecting the elements of the correlation matrix in Eqn. (4.4). The first column is clearly linearly independent from the rest due to the $(1,1)$ matrix element: $r_{11} = 1$. By looking at the matrix elements r_{22}, r_{23}, r_{42}, and r_{43}, it can be assumed that the second and fourth columns in Eqn. (4.4) are linearly independent:

$$\begin{pmatrix} r_{22} & r_{42} \\ r_{23} & r_{43} \end{pmatrix} = \begin{pmatrix} -0.34 & 0.25 \\ 0.38 & 0.26 \end{pmatrix}, \tag{4.5}$$

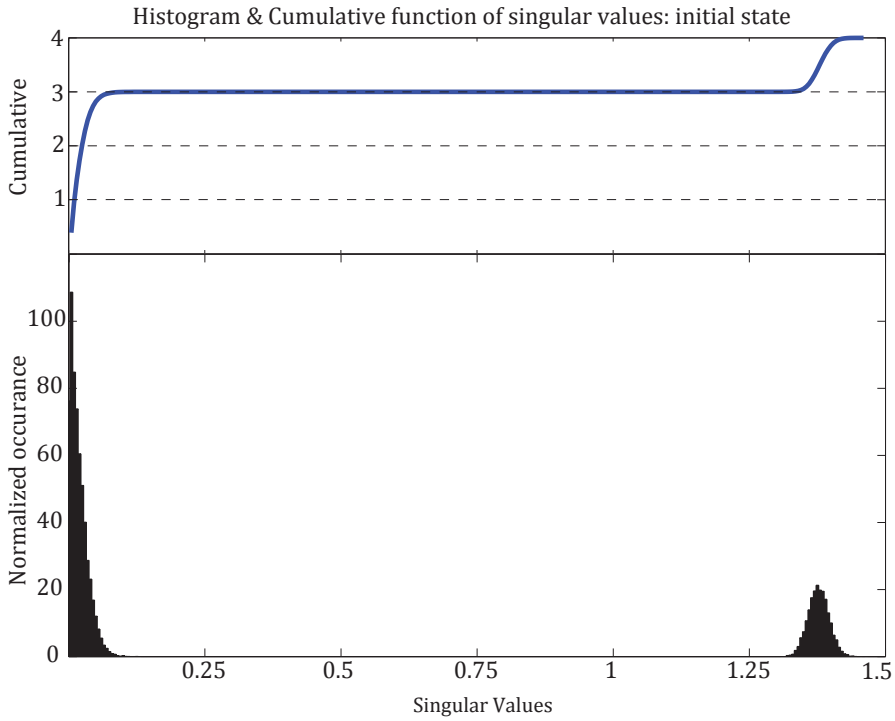

Figure 4.4: Histogram of singular values from the initial state correlation matrix. This histogram was generated by Monte Carlo sampling from the errors of a randomly chosen 4×4 truncated correlation matrix. Errors on each of 1000 R_{trunc} were sampled 10 times, and the bin size of the histogram is 0.005. We used the truncated correlation matrices in order to reduce the compounding of errors during the calculation of singular values. The cumulative of the distribution is plotted to assist the reader in determining the rank. Here, there are clearly three singular values consistent with zero and one non-zero singular value. The conclusion drawn from this data is that the rank is very likely 1 and most certainly less than the 3 required to detect discord.

which leads to a rank of at least three. Indeed, checking this assumption by performing the same form of Monte Carlo sampling as used on the initial state, the rank of the truncated correlation matrix was determined to be at least three. Because only four columns of the correlation matrix were measured, the 10000 values sampled in the Monte Carlo were only for this instance of the truncated correlation matrix (unlike the 1000 truncated correlations matrices that were sampled from in the initial state analysis). The histogram of singular values is given in Figure 4.5, including the cumulative of the distribution to assist in determining the rank. The data clearly indicates that there is one singular value consistent with zero, two singular values in the middle, and another non-zero singular value around one.

4.4 Discussion and Conclusion

While quantum discord is a good measure of the non-classical correlations present in a quantum system, it is very difficult to measure the quantum discord for a generic system since full tomographic data is required. As an alternative, it is possible to measure the existence of non-classical correlations, as measured by the quantum discord, using a discord witness. In this experiment, we set out to witness quantum correlations in the highly mixed states of liquid state NMR that are found in the DQC1 algorithm. The particular witness used was proposed by Dakic, Vedral and Brukner [DVB10], and works for generic states of arbitrary dimension.

We know that the states in our NMR experiments cannot contain entanglement due to their very small polarization, but it has been theoretically calculated that quantum discord can exist in DQC1 algorithms that have non-zero polarization. In simulation, we show that for the polarization of 1.43×10^{-5} in our experiment, the quantum discord is approximately 5.4×10^{-11}, and in this chapter, we set out to determine whether or not it is possible to measure such a small amount of non-classical correlations. In order to detect correlations of that size in our experiment, we show that detecting correlations in the pseudopure state ρ_{pps} is necessary and sufficient to detect correlations in the physical NMR state ρ_{NMR}.

In order to detect quantum correlations in the state

$$\rho = \sum_{n,m} r_{nm} A_n \otimes B_m,$$

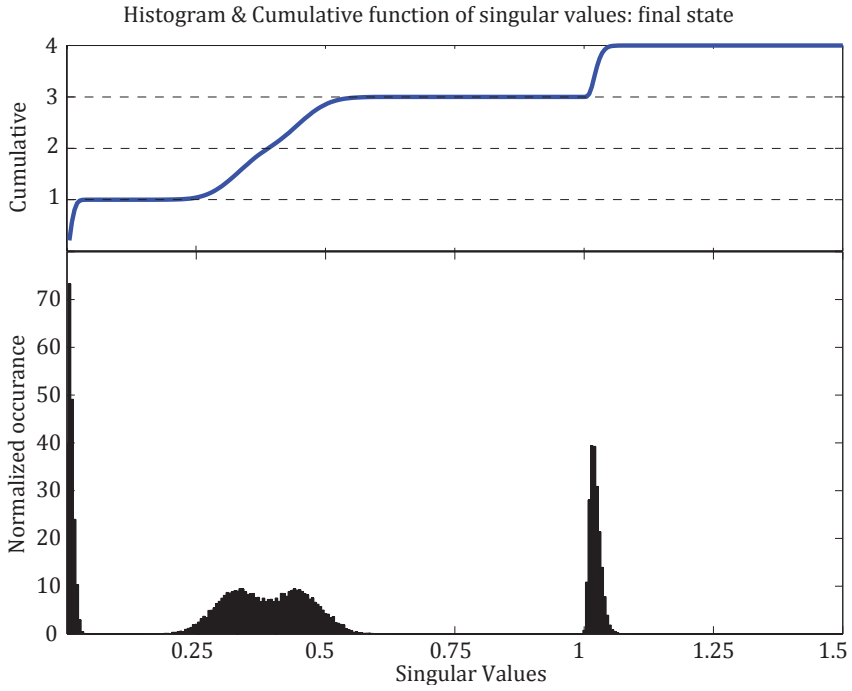

Figure 4.5: Distribution of the singular values and the cumulative distribution computed for the experimentally determined correlation matrix of the final state of a DQC1 algorithm implemented in NMR. This distribution is created by sampling from a normal distribution of the errors on each matrix element and calculating the singular values of the sampled matrix. There are 10,000 samples in this plot and the histogram bin size is 0.005. The cumulative of the distribution is included to guide the reader in estimating the integral of portions of the distribution. With certainty, we deduce that the final state has a rank of at least three, indicating that quantum discord is detected in this state. Discord is detected in the pseudopure state ρ_{pps}, indicating the that physical state, $\rho_{NMR} = (1-\alpha)I/2^N + \alpha\rho_{pps}$ also has non-zero discord, regardless of the polarization α.

where r_{nm} are the matrix elements of correlation matrix R, we need to find that Rank$(R) > dim(A)$. In our case, system A consists of a single qubit. We measure the rank of the correlation matrix in the pseudopure state at the initial and final points of the DQC1 algorithm. The experimental results given in Section 4.3 show that the rank of correlation matrix R in the initial state of the DQC1 algorithm is one and the final state has a rank of at least three. Therefore, while we were not able to detect discord in the initial state of the DQC1 algorithm, we successfully witnessed non-classical correlations in the final state. This is despite the fact that these correlations are on the order of 10^{-11}. These results are consistent with quantum discord being generated in the DQC1 algorithm, and support the idea that it may be the source of the speedup over the best classical algorithms.

There are still many unanswered questions in the quest to understand the non-classical nature of the DQC1 model. Since we know that almost all quantum states contain non-zero discord, an interesting question is whether or not there is a threshold value for non-classical correlations, such that any correlations above that give rise to 'useful' quantum effects? And is there a way to efficiently measure the quantum correlations in the DQC1 algorithm, or perhaps bound their amount? We tackle the latter question in Chapter 5.

Chapter 5

Analyzing Discord in the DQC1 Model of Computation

As we have previously discussed in this thesis, the DQC1 model of computation is of great interest in the quantum information community. We know that for the most natural bipartite splitting, between the top and bottom register, there is never any entanglement, yet there are quantum correlations measured by the quantum discord. It is possible to numerically solve for the value of these correlations once given full tomographic data, and in the absence of that, we can detect the presence of these correlations (Chapter 4). However, because almost all quantum states contain non-zero quantum discord [FAC+10], it is desirable to have an experimentally suitable method for measuring the magnitude of the correlations.

In this chapter we describe how it is possible to measure quantum correlations in a DQC1-state. This is achieved using the measure of quantum correlations known as the geometric quantum discord (GQD) [DVB10] (to be explained in Section 5.2.1), which can be analytically solved for a DQC1-state. We also show that solving for the geometric discord in a DQC1-state is in the complexity class DQC1. In other words, in order to solve for the GQD, you only need to perform a DQC1 algorithm. Specifically, a DQC1 algorithm where the controlled-unitary is applied twice. This work is given in Section 5.2, and an experimental measurement of the GQD of an NMR implementation of the DQC1 model is detailed in Section 5.3.

In addition to this result, which holds for any size DQC1-state, for the special case

of a two-qubit DQC1 algorithm, an analytical expression for the quantum discord (QD) based on mutual information is found. Calculating the QD for a two-qubit DQC1 state also only requires the result of the DQC1 algorithm (namely, the trace of the unitary). This work is outlined in Section 5.4. Finally, we end this chapter with a conclusion in Section 5.5. The results given in this chapter have been published in Physical Review A [PML12], copyright (2012) by the American Physical Society. The author of this thesis performed the experiment and the mathematical calculations. The ideas, methodology, and discussion were done in collaboration with O. Moussa.

5.1 Background: Discord and DQC1

5.1.1 Previous work analyzing the Quantum Discord

Analytical expressions for the QD are desirable since computing the QD directly from its definition is computationally intensive, as in addition to requiring full knowledge of the state it requires an optimization over all possible projective measurements acting on one of the subsystems. In the next section we will focusing on DQC1-states, but first let us briefly describe some of the progress for creating a closed form equation for the quantum discord of special sets of states.

- In 2008, Luo [Luo08] analytically studied the discord of a set of two-qubit states that can be written as $\rho_{bd} = 1/4(I + \sum_i c_i \sigma_i \otimes \sigma_i)$, known as Bell-diagonal states or states with maximal mixed marginals. The quantum discord for this set of states is

$$D(\rho_{bd}) = \sum_{i,j=0}^{1} \lambda_{ij} \log 4\lambda_{ij} - \mathcal{C}(\rho_{bd}),$$

  where $\mathcal{C}(\rho)$ is the value of classical correlations as defined by Henderson and Vedral [HV01] and is equal to $1/2 \sum_{i=0}^{1}(1 + (-1)^i c) \log(1 + (-1)^i c)$, for $c = \max(c_i)$.

- The quantum discord for two parameters states of $2 \times d$ dimension was found in Ref. [Ali10]. The two (real) parameter state is defined as

$$\rho_{\delta,\gamma} = \delta \sum_{i=0}^{1} \sum_{j=2}^{d-1} |ij\rangle\langle ij| + \beta(|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+|) + \gamma|\psi^-\rangle\langle\psi^-|,$$

where $|ij\rangle$ is an orthonormal basis for the $2 \times d$ system, $|\phi^{\pm}\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle)$ and $|\psi^{\pm}\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$ are the Bell states, and β is a dependent variable by requiring $\mathrm{Tr}(\rho_{\delta,\gamma}) = 1 = 2(d-2)\alpha + 3\beta + \gamma$. Then the quantum discord of this state is equal to

$$D(\rho_{\delta,\gamma}) = \beta \log(2\beta) + \gamma \log 2\gamma - (\beta + \gamma) \log(\beta + \gamma).$$

It has been shown that any bipartite state of dimension $2 \times d$ can be written in the form $\rho_{\delta,\gamma}$ using local operations and classical communication [CL03]. Note that while the discord does not change under local unitary operations, it can both increase and decrease when you use classical communication in addition to local operations.

- The set of two-qubit states with an analytical expression for the discord grew in 2010 and 2011 when the set of two qubit X-states were added [ARA10, CZY$^+$11]. True to their name, X-states can be written in the computational basis as

$$\rho_X = \begin{pmatrix} \rho_{00} & 0 & 0 & \rho_{03} \\ 0 & \rho_{11} & \rho_{12} & 0 \\ 0 & \rho_{12}^* & \rho_{22} & 0 \\ \rho_{03}^* & 0 & 0 & \rho_{33} \end{pmatrix}.$$

- In 2011 the optimal measurements to measure an upper bound on the discord of two-qubit states was found [LMXW11]. Using the so-called maximal-correlation-direction measurement (MCDM), they prove that for zero-discord states and those with maximally mixed marginals, this MCDM is optimal. For all other two-qubit states, the MCDM gives an upper bound on the quantum discord present.

- Analytical progress on computing the quantum discord of general two-qubit states has been made [GA11c], where the solution can be found by solving a set of transcendental equations.

While all of this progress is promising, there is still no efficient method for calculating the discord of a general quantum state.

5.1.2 Discord for an average DQC1-state: analytical and numerical

Let us shift our focus to the DQC1 model of computation, where Datta et al. [DSC08] found an expression for the average discord in the state at the conclusion of the DQC1 model (what we hereafter refer to as the DQC1-state). The result is

$$D_{avg}(\rho_{DQC1}) = 2 - H_2\left(\frac{1-\alpha}{2}\right) - \log(1+\sqrt{1-\alpha^2}) - (1-\sqrt{1-\alpha^2})\log e,$$

with the assumptions that the number of qubits in the bottom register is large and that the unitaries are chosen randomly from the Haar measure. They compare the average given by the above expression with a numerically found average and show that the above expression is a good estimate once the number of qubits in the bottom register reaches five.

After reading the work of Datta et al., we were very curious as to the spread of the quantum discord for systems with a small number of qubits. Figures 5.1 and 5.2 show numerical results for the discord in a DQC1-state where the unitary was chosen randomly from the Haar measure, as a function of the polarization. Note that all graphs in Figures 5.1-5.2 have been plotted with the same scale on the vertical axis to allow for easier comparison. We simulated a random unitary from the Haar measure in systems whose bottom register has between one and six qubits. We found that the spread of the discord in the DQC1-state (referred to as ρ_{DQC1}) decreases rapidly as the number of qubits in the bottom register grows.

These figures suggest that as the dimension of the bottom register grows, the discord in the average case is less likely to be near zero. However, we know that there are unitaries that give rise to zero quantum discord in the DQC1 model: Dakic, Vedral and Brukner [DVB10] found that unitary transformations of the form $U = e^{i\theta}A$, where $A^2 = I$ give rise to zero discord in the final DQC1 state[1]. So that begs the question: what about the discord of the states after unitary transformations that are very close to a 'zero-discord' unitary, such as the identity? To study this, we numerically look at the DQC1-states that arise from controlled-unitaries that have a less than perfect fidelity with the identity. The gate fidelity measure used is defined as

$$F(U_1, U_2) = \frac{|\mathrm{Tr}(U_1 U_2^\dagger)|^2}{d^2},$$

[1]Note that there is a typographical error in the published version of the paper where they incorrectly state that the binary observable has $A^2 = A$. (Ref. [DVB10])

where d is the dimension of the unitary. The plot in Figure 5.3 shows the discord for a DQC1-state when the controlled-unitary has been generated to have a fidelity of between 0.86 and 0.99 with the identity[2].

This figure indicates that, while the data in Figures 5.1 and 5.2 have a gap between zero discord and the average for the DQC1-state as the dimension gets larger, this is a consequence of the concentration of measure for Haar random unitary matrices, rather than a property of the discord. It indicates that, while we can mathematically say that most unitaries in the DQC1 model will give rise to values of quantum discord close to the average, it does not give us any indication of the amount of discord present in a particular DQC1 experiment. This is one of the reasons that we search for an analytical expression for the amount of non-classical correlations present in the DQC1 model in Sections 5.2 and 5.4.

[2]Fidelities of 0.99 are important to the NMR experimental implementations in this thesis, as we have simulated the fidelity of the four-qubit DQC1 controlled-unitaries to be implemented at approximately 0.99 fidelity (described in Appendix A).

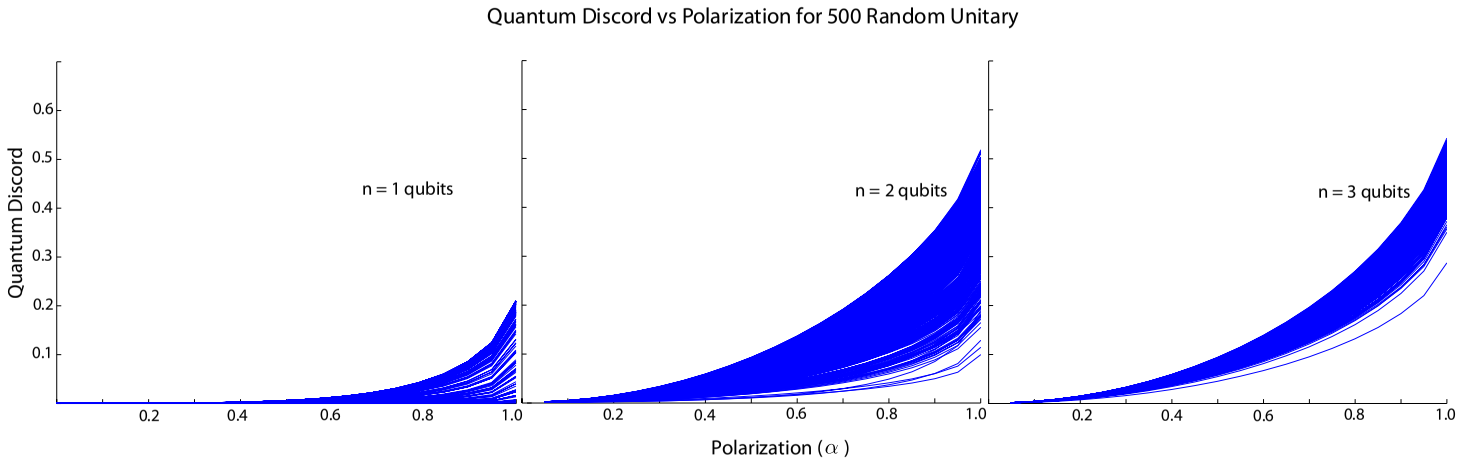

Figure 5.1: These graph shows the quantum discord for the DQC1-state generated by a unitary randomly chosen according to the Haar measure. The graphs plotted here have $n = 1$, 2, and 3 qubits in the bottom register and all plots have the same scale on the vertical axis. It can be seen that as the number of qubits in the bottom register increase, the standard deviation in the average quantum discord decreases. This is due, not to the measure of quantum discord, but to the concentration of the Haar measure.

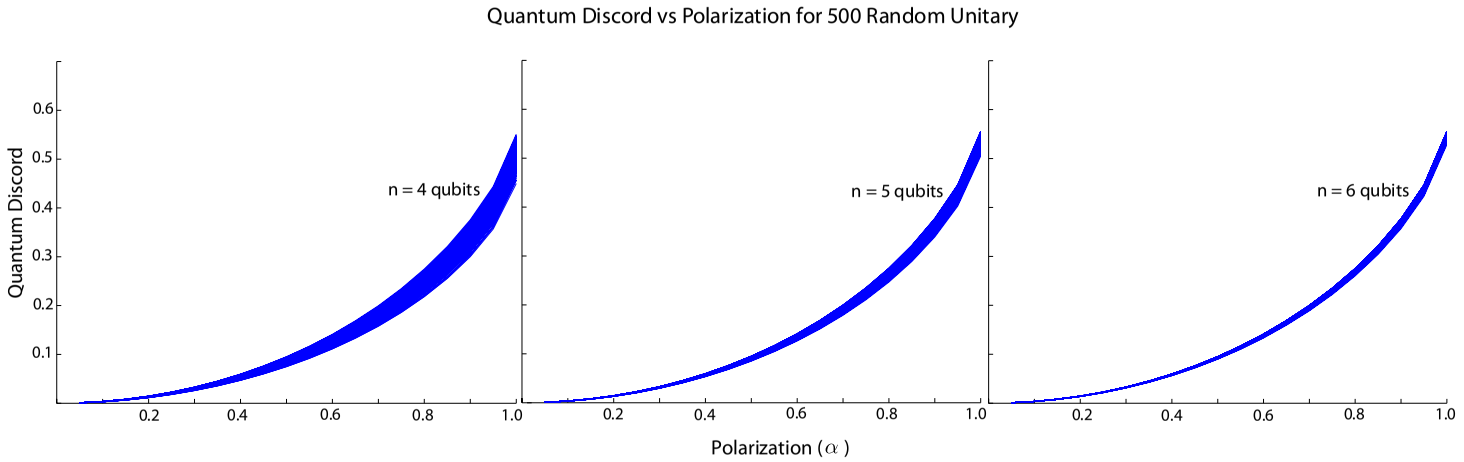

Figure 5.2: These graphs are the same as those in Figure 5.1 but for 4, 5, and 6 qubit in the bottom register.

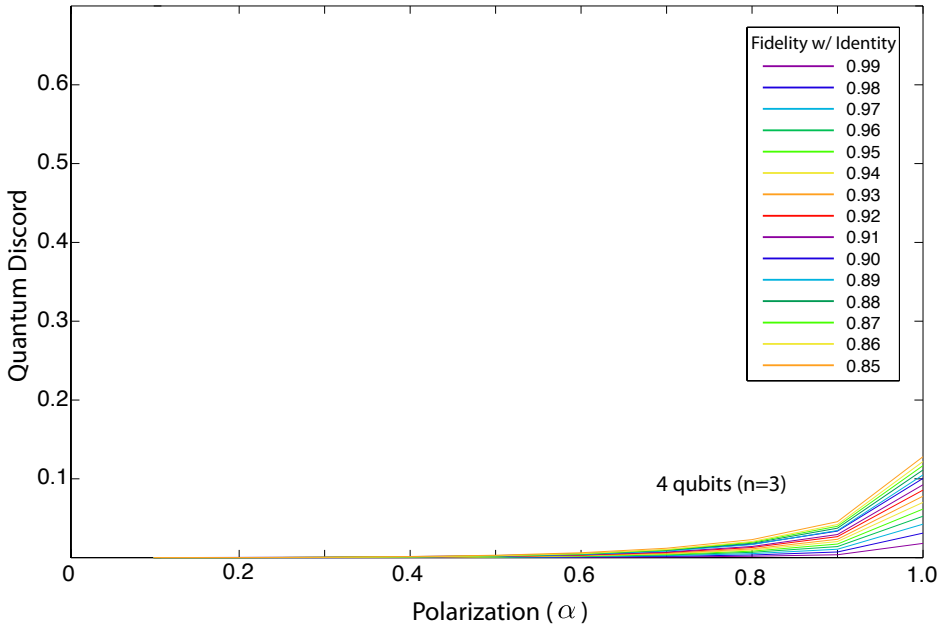

Figure 5.3: The quantum discord for a four-qubit DQC1-state after application of a controlled-unitary designed to have a fidelity of between 0.85 and 0.99 with the identity. This confirms our suspicion that the gap from zero quantum discord and the mean value in the 'typical' instances shown in Figures 5.1 and 5.2 is due to concentration of the Haar measure, and is not a feature of the quantum discord of DQC1-states.

5.2 Geometric Discord of a DQC1-state

Until this point, we have concentrated on the quantum discord as a measure of quantum correlations. We have come to realize that while QD is a very good measure of the correlations in a state, it is extremely hard to measure. As mentioned in Section 5.1, work to find analytical expressions for two qubit states have been tedious, and successful for only a handful of states. This motivated Dakic, Vedral and Brukner [DVB10] to define a different measure of quantum correlations called the geometric quantum discord (GQD). Directly from their definition, with a relatively small amount of analysis, they were able to provide an analytical expression for the GQD in an arbitrary two qubit state – an accomplishment yet to be achieved in the case of quantum discord.

In this section we look at this measure of correlations in more detail, specifically for the states present at the conclusion of the DQC1 algorithm. We are able to find an analytical expression for the quantum discord of these states, which is contained in the complexity class DQC1. That is to say that it is easily measured by a DQC1 algorithm. This section proceeds as follows: in Section 5.2.1 we explain the measure of GQD and review the existing literature. Section 5.2.2 is devoted to solving for an analytical expression for the geometric discord for an arbitrary DQC1-state. In Section 5.2.3 we discuss these results and look at the geometric discord for an average unitary, analogous to the work presented in Section 5.1.2. Moving to Section 5.3, we report the results of an experiment to measure the geometric discord in a four-qubit DQC1-state.

5.2.1 Geometric quantum discord as a measure of quantum correlations

The geometric quantum discord [DVB10] is defined as the minimum norm distance between the given state and the set of zero-discord states:

$$D_G^A(\rho) = \min_{\chi \in \Omega_0^A} ||\rho - \chi||^2 \tag{5.1}$$

where Ω_0 is the set of all classical-quantum, zero discord ($D(A:B) = 0$) states, parameterized by $\Omega_0^A = \sum_j p_j |j\rangle\langle j| \otimes \rho_j^B$. The quantity $||\rho - \chi||^2 = \mathrm{Tr}(\rho - \chi)^2$ is the square of the Hilbert-Schmidt norm of Hermitian operators. Note that the GQD (just like the QD), is not symmetric in the subsystems, as $D_G^B(\rho) = \min_{\chi \in \Omega_0^B} ||\rho - \chi||^2$, where $\Omega_0^B = \sum_j p_j \rho_j^A \otimes |j\rangle\langle j|$.

Dakic, Vedral and Brukner were able to provide a closed form expression for the geometric discord of arbitrary two-qubit states. They start by writing an arbitrary two-qubit state as

$$\rho = \frac{1}{4}\left(I \otimes I + \sum_{i=1}^{3} x_i \sigma_i \otimes I + \sum_{i=1}^{3} y_i I \otimes \sigma_i + \sum_{i,j=1}^{3} T_{ij} \sigma_i \otimes \sigma_j \right), \tag{5.2}$$

where $x_i = \mathrm{Tr}(\rho \sigma_i \otimes I)$, $y_i = \mathrm{Tr}(\rho I \otimes \sigma_i)$, and $T_{ij} = \mathrm{Tr}(\rho \sigma_i \otimes \sigma_j)$. Then the geometric discord for this two-qubit state can be written as

$$D^A_{G2}(\rho) = \frac{1}{4}\left(||\vec{x}||^2 + ||T||^2 - k_{max} \right), \tag{5.3}$$

where k_{max} is the largest eigenvalue of the matrix $K = \vec{x}\vec{x}^{\top} + TT^{\top}$. This expression was found to be valid for states with dimension $2 \times d$ in Ref. [VR11], where the state is now defined by

$$\rho = \frac{1}{2d}\left(I + \sum_{i=1}^{3} x_i \sigma_i \otimes I + \sum_{i=1}^{d^2-1} y_i I \otimes O_i + \sum_{i=1}^{3} \sum_{j=1}^{d^2-1} T_{ij} \sigma_i \otimes O_j \right), \tag{5.4}$$

where O_j is a basis of $(d^2 - 1)$ linearly independent operators, and $\vec{x}$, $\vec{y}$, and T are defined as above, with O_j in place of the Pauli matrices on the d-dimensional system.

While the existence of a closed form expression is a great improvement over other measures, there is no intuitive way to measure the geometric discord without full tomography. This prompted Girolami and Adesso [GA11b] to propose a closely related measure that is a lower bound to the GQD, and is written in terms of observables for two-qubit states. They are able to extend their approach to larger systems, but the procedure is non-trivial and very involved. Whereas, the analytical expression for the geometric discord for DQC1-states given in the following section is a very elegant solution that does not change with the system size, and only requires the implementation of the DQC1 algorithm to quantify the GQD.

Shortly after the measure of geometric quantum discord was introduced, Luo and Fu [LF10] showed that it is equivalent to

$$D^A_G(\rho) = \min_{\Pi^A} ||\rho - \Pi^A(\rho)||^2, \tag{5.5}$$

where $\Pi^A(\rho) = \sum_k (\Pi^A_k \otimes I)\rho(\Pi^A_k \otimes I)$, and $\Pi^A = \{\Pi^A_k\}$ is a projective measurement on system A. That is to say that it is sufficient to consider the minimization over projective

measurements. Likewise, $D_G^B(\rho) = \min_{\Pi^B} ||\rho - \Pi^B(\rho)||^2$, where Π^B is a projective measurement on system B. It is this expression for the quantum discord that we use to find the analytical solution for DQC1-states.

Geometric discord has been extensively researched in the past couple of years. Studies have been done on the properties of GQD and how it relates to the quantum discord based on mutual information [BPPC11, GA11c]. The GQD has been studied for Gaussian states [AG11], qubit-qutrit systems under dephasing [KG11], and has been compared to other measures of correlations [GA11a]. In addition to the proposal to measure a lower bound for the geometric discord of $2 \times d$ states mentioned above ([GA11b]), there exists a proposal to directly measure the geometric discord for the set of two-qubit states [JZYS11].

5.2.2 Analytical expression for the Geometric discord of a DQC1-state

In order to arrive at an analytical expression for the GQD of a DQC1-state, we must perform a minimization over all possible projective measurements. We will be looking at the geometric discord where the measurement is performed on the single qubit subsystem. The GQD from Eqn. (5.5) can be written as

$$\begin{aligned} D_G^A(\rho) &= \min_{\Pi^A} ||\rho - \Pi^A(\rho)||^2 \\ &= \min_{\Pi^A} (\mathrm{Tr}(\rho^2) - 2\mathrm{Tr}(\rho\Pi^A(\rho)) + \mathrm{Tr}(\Pi^A(\rho)^2)). \end{aligned} \tag{5.6}$$

The final state of a DQC1 algorithm (given in Eqn. (2.27)) is

$$\rho_{DQC1} = \frac{1}{2^{n+1}} \begin{pmatrix} I^{\otimes n} & \alpha U_n^\dagger \\ \alpha U_n & I^{\otimes n} \end{pmatrix}, \tag{5.7}$$

where n is the number of qubits in the bottom register. We will parameterize the measurements as $\Pi_\pm^A = |\psi_\pm\rangle\langle\psi_\pm|$, where $|\psi_+\rangle = a|0\rangle + be^{i\phi}|1\rangle$ and $|\psi_-\rangle = b|0\rangle - ae^{i\phi}|1\rangle$, so that the state after a measurement is

$$\begin{aligned} \Pi^A(\rho_{DQC1}) &= (|\psi_+\rangle\langle\psi_+| \otimes I_n)\, \rho_{DQC1}\, (|\psi_+\rangle\langle\psi_+| \otimes I_n) + (|\psi_-\rangle\langle\psi_-| \otimes I_n)\, \rho_{DQC1}\, (|\psi_-\rangle\langle\psi_-| \otimes I_n) \\ &= \frac{1}{2^{n+1}} \begin{pmatrix} I_n + \alpha ab(a^2 - b^2)(e^{-i\phi}U + e^{i\phi}U^\dagger) & 2\alpha a^2 b^2 (e^{-2i\phi}U + U^\dagger) \\ 2\alpha a^2 b^2 (U + e^{2i\phi}U^\dagger) & I_n - \alpha ab(a^2 - b^2)(e^{-i\phi}U + e^{i\phi}U^\dagger) \end{pmatrix}, \end{aligned}$$

where we have used the fact that $a^2 + b^2 = 1$.

We can now immediately calculate each term in Eqn. (5.6). The first term, the purity of the state of the total system, is invariant under unitary transformations. Therefore, it can be calculated for the initial state, and only depends on the initial polarization of the top register:

$$\mathrm{Tr}(\rho_{DQC1}^2) = \frac{1+\alpha^2}{2^{n+1}}. \tag{5.8}$$

The second term is as follows:

$$\begin{aligned}\mathrm{Tr}(\rho_{DQC1}\Pi^A(\rho_{DQC1})) &= \frac{1}{2^{2n+1}}\left(\alpha^2a^2b^2\mathrm{Tr}(e^{2i\phi}U^{\dagger 2}+e^{-2i\phi}U^2)+(2\alpha^2a^2b^2+1)2^n\right)\\ &= \frac{\alpha^2a^2b^2}{2^{2n+1}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2}+e^{-2i\phi}U^2)+\frac{2\alpha^2a^2b^2+1}{2^{n+1}},\end{aligned}$$

and turns out to be equal to $\mathrm{Tr}(\Pi^A(\rho_{DQC1})^2)$, the third term. Then, the expression for the geometric quantum discord of the DQC1 state simplifies to

$$D_G^A(\rho_{DQC1}) = \min_{\Pi^A}\left(\frac{1+\alpha^2}{2^{n+1}} - \frac{\alpha^2a^2b^2}{2^{2n+1}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2}+e^{-2i\phi}U^2) - \frac{2\alpha^2a^2b^2+1}{2^{n+1}}\right). \tag{5.9}$$

In order to find the minimum GQD, we must maximize the function

$$f(a,\phi) = \frac{\alpha^2a^2b^2}{2^{2n+1}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2}+e^{-2i\phi}U^2)+\frac{2\alpha^2a^2b^2+1}{2^{n+1}}, \tag{5.10}$$

since it comes into the equation for the geometric discord with a negative sign.

Let us start by setting the partial derivatives of parameters a and ϕ (noting that $b = \sqrt{1-a^2}$) to zero. For the partial derivative with respect to a, we find that

$$\begin{aligned}\frac{\partial f}{\partial a} &= 0\\ &= \frac{2\alpha^2a(1-2a^2)}{2^{2n+1}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2}+e^{-2i\phi}U^2)+\frac{4\alpha^2a(1-2a^2)}{2^{n+1}},\end{aligned}$$

leading to the solution $a_0 = 1/\sqrt{2}$. Note that $a = 0$ is also a valid solution, and is ruled out in Appendix B. In addition, the equation above could be satisfied if $\mathrm{Tr}(e^{2i\phi}U^{\dagger 2}+e^{-2i\phi}U^2) = -2^{n+1}$, however, this is not possible since the trace can only have a value between -2^n and 2^n.

Now, let us determine the value of ϕ by setting the partial derivative with respect to ϕ to zero:

$$\begin{aligned} \frac{\partial f}{\partial \phi} &= 0 \\ \Rightarrow \frac{\partial}{\partial \phi}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) &= 0, \end{aligned}$$

assuming $a \neq 0$ and $b \neq 0$, which are shown in Appendix B. In order to solve for the value of ϕ, we express the unitary in terms of its eigen-decomposition: $U = \sum_j e^{i\theta_j}|\theta_j\rangle\langle\theta_j|$. Then the trace can be written as

$$\begin{aligned} \mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) &= \mathrm{Tr}\left(e^{2i\phi}\sum_j e^{-2i\theta_j}|\theta_j\rangle\langle\theta_j| + e^{-2i\phi}\sum_j e^{2i\theta_j}|\theta_j\rangle\langle\theta_j|\right) \\ &= \sum_j (e^{2i(\phi-\theta_j)} + e^{-2i(\phi-\theta_j)}) \\ &= \sum_j 2\cos(2(\phi-\theta_j)). \end{aligned} \tag{5.11}$$

The minimization procures reduces to

$$\begin{aligned} 0 &= \frac{\partial}{\partial \phi}\sum_j (\cos(2(\phi-\theta_j))) \\ &= \frac{\partial}{\partial \phi}\left(\sum_j 2\cos^2(\phi-\theta_j) - 1\right) \\ &= \sum_j 4(\cos(\phi-\theta_j)\sin(\phi-\theta_j)) \\ &= \sum_j 2\sin(2(\phi-\theta_j)) \\ &= \sum_j 2\Big(\sin(2\phi)\cos(2\theta_j) - \cos(2\phi)\sin(2\theta_j)\Big) \\ \Rightarrow \frac{\sin(2\phi)}{\cos(2\phi)} &= \frac{\sum \sin(2\theta_j)}{\sum \cos(2\theta_j)} = \frac{\mathrm{Im}(\mathrm{Tr}(U^2))}{\mathrm{Re}(\mathrm{Tr}(U^2))} \\ \Rightarrow \phi &= \frac{1}{2}\arctan\left(\frac{\mathrm{Im}(\mathrm{Tr}(U^2))}{\mathrm{Re}(\mathrm{Tr}(U^2))}\right). \end{aligned}$$

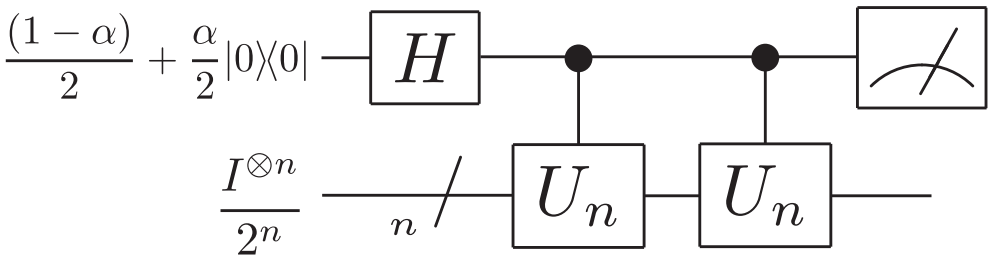

Figure 5.4: This circuit diagram shows the modified DQC1 algorithm that yields $\alpha \mathrm{Tr}(U^2)/2^n$ upon measurement of $\langle\sigma_x\rangle + i\langle\sigma_y\rangle$. This experiment allows us to find the optimal value of ϕ_0 to minimize the geometric discord.

Thus, the optimal values for a and ϕ are

$$a_0 = \frac{1}{\sqrt{2}} \rightarrow b_0 = \frac{1}{\sqrt{2}} \tag{5.12}$$

$$\phi_0 = \frac{1}{2}\arg(\mathrm{Tr}(U^2)). \tag{5.13}$$

These values are confirmed to correspond to a minimum GQD in Appendix B.

It is possible (although unnecessary) to experimentally determine the value of ϕ_0 by performing a DQC1 algorithm. The circuit required can be seen in Figure 5.4, where we have applied the controlled-unitary twice. Then, by performing the standard DQC1 measurement ($\langle\sigma_x\rangle$ and $\langle\sigma_y\rangle$), the trace of the unitary squared can be easily measured.

Now that we have found the optimal measurement basis, let us simplify the expression for the geometric discord of the $2 \times n$ DQC1 state:

$$D_G^A(\rho_{DQC1}) = \left(\frac{\alpha}{2}\right)^2 \frac{1}{2^{2n}} \left[2^n - \mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2)\right] \tag{5.14}$$

$$= \left(\frac{\alpha}{2}\right)^2 \frac{1}{2^{2n}} \left[2^n - \sum_j \cos(2(\phi_0 - \theta_j))\right]. \tag{5.15}$$

The final term in Eqn. (5.15) for the geometric discord can be determined by performing a modified DQC1 algorithm, where a rotation,

$$R = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi_0} \end{pmatrix}, \tag{5.16}$$

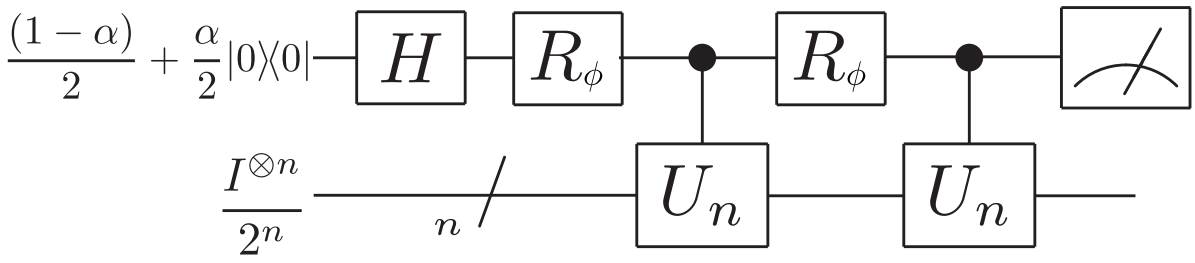

Figure 5.5: This circuit diagram shows that modified DQC1 algorithm that is used to solve for $\sum_j \cos(2(\phi - \theta_j))$. The angle of rotation is determined by a previous DQC1 experiment where $\mathrm{Tr}(U^2)$ was found. This allows us to experimentally determine the value for the geometric discord in a DQC1 state.

is performed on the top qubit before the controlled unitary. By performing the rotation and the controlled unitary twice back-to-back (as shown in Figure 5.5), a measurement of $\langle\sigma_x\rangle$ will yield the desired result, since the final state of this circuit is

$$\rho_{\phi^2} = \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha e^{2i\phi_0} U^{\dagger 2} \\ \alpha e^{-2i\phi_0} U^2 & I_n \end{pmatrix}, \tag{5.17}$$

and a measurement of $\langle\sigma_x\rangle$ gives

$$\langle\sigma_x\rangle = \frac{\alpha}{2^n} \sum_j \cos(2(\phi_0 - \theta_j)). \tag{5.18}$$

Although we are able to solve for the geometric discord with a DQC1 computation, it turns out that experimentally, we do not need to perform the circuit given in Figure 5.5, as the rotation can be 'virtually' performed. Since the rotation commutes with the controlled unitary, it can be combined with the measurement at the conclusion of the algorithm. We can directly see this by writing $\mathrm{Tr}(U^2) = re^{i\eta}$, where $r = |\mathrm{Tr}(U^2)|$ and $\eta = \arg(Tr(U^2)) = 2\phi_0$. This greatly simplifies our expression for the GQD. Looking at $\sum_j \cos(2(\phi_0 - \theta_j))$

from Eqn. (5.15), we see that

$$\sum_j \cos(2(\phi_0 - \theta_j)) = \frac{1}{2}\mathrm{Tr}(e^{2i\phi_0}U^{\dagger 2} + e^{-2i\phi_0}U^2) \text{ (from Eqn. (??))} \quad (5.19)$$

$$= \frac{1}{2}\left(e^{2i\phi_0}\mathrm{Tr}(U^{\dagger 2}) + e^{-2i\phi_0}\mathrm{Tr}(U^2)\right) \quad (5.20)$$

$$= \frac{r}{2}\left(e^{i(2\phi_0-\eta)} + e^{-i(2\phi_0-\eta)}\right) \quad (5.21)$$

$$= \frac{r}{2}(2) = |\mathrm{Tr}(U^2)|. \quad (5.22)$$

The simplified equation for the geometric quantum discord of a DQC1-state is then

$$D_G^A(\rho_{DQC1}) = \left(\frac{\alpha}{2}\right)^2 \frac{1}{2^{2n}}\left[2^n - |\mathrm{Tr}(U^2)|\right] \quad (5.23)$$

$$= \left(\frac{\alpha}{2}\right)^2 \frac{1}{2^n}\left[1 - \tau_2\right], \quad (5.24)$$

where $\tau_2 = |\mathrm{Tr}(U^2)|/2^n$ and goes from 0 to 1. Therefore, the GQD of a DQC1-state can be measured by a DQC1 circuit with back-to-back unitaries found in Figure 5.4. This indicates that the geometric quantum discord of a DQC1-state has a minimum value of 0 and a maximum value of $\alpha^2/2^{n+2}$, where α is the polarization of the top qubit in the DQC1 model.

5.2.3 Discussion

Above we have found an analytical expression for the geometric discord for a generic DQC1-state that only depends on the absolute value of the trace of the unitary squared. This value is easily determined by implementing a DQC1 algorithm. In this section we will discuss this result and the implications it has for both the measure of geometric quantum discord and the DQC1 model of computation.

- Solving for the GQD of a DQC1-state is a problem in the complexity class DQC1. This means that it can be solved on the model of computation that has a single bit of quantum information available for computation, n completely mixed qubits, and a classical computer, with the same conditions on the unitaries as described in the DQC1 class.

- The optimal measurement has $a_0 = 1/\sqrt{2}$, independent of the unitary. This indicates that the measurement is always in the x–y plane (transverse plane in the Bloch sphere), which is the measurement performed in DQC1 algorithms. The phase ϕ_0 of the optimal measurement does depend on the unitary, and while it is possible to measure on a DQC1 quantum information processor, is not necessary to experimentally perform, as we only need the magnitude of the trace to solve for the GQD.

- The amount of geometric discord in a DQC1-state scales quadratically with the polarization of the top qubit. When looking for entanglement in a DQC1-state, the value of the polarization is very important. In fact, when the polarization drops below 0.5, entanglement has never been found [DFC05]. Datta et al. showed that for the quantum discord measure of non-classical correlations, there was a decrease in the correlations with a decrease in polarization, but only a zero value for the polarization gave rise to zero quantum discord [DSC08]. This is exactly what we found here: decreasing the polarization does not eliminate the GQD completely, but it does decrease the quantity. In addition, as expected, we find that zero polarization gives rise to zero geometric quantum discord.

- The GQD of DQC1-states does not depend on the eigenvectors of U, but rather the distribution of eigenphases θ_j. This makes it possible to examine classes of unitaries that give rise to the same GQD. For example, the unitaries that give rise to zero GQD (and hence, QD) require $|\mathrm{Tr}(U^2)| = 2^n$:

$$
\begin{aligned}
|\mathrm{Tr}(U^2)| &= \left|\sum_{j=1}^{2^n} e^{2i\theta_j}\right| && (5.25)\\
&\Rightarrow\ e^{2i\theta_j} = e^{i\xi}1,\ \forall\, j,\ \text{and any value of } \xi && (5.26)\\
&\Rightarrow\ 2\theta_j = \xi \pm 2\pi,\ \forall\, j && (5.27)\\
&\Rightarrow\ U = e^{i\xi/2}\sum_{j=1}^{2^n} e^{\pm i\pi}|j\rangle\langle j| && (5.28)\\
U &= e^{i\xi/2}A, && (5.29)
\end{aligned}
$$

  where A is a binary observable ($A^2 = I$). Note that this derivation gives rise to the same result for unitaries leading to zero QD in DQC1 in Ref. [DVB10], where they note that this is evidence that contradicts the idea that QD is the cause of the quantum advantage in the DQC1 model.

- On the other hand, there exists a set of unitaries whose trace can be efficiently estimated on a classical computer, yet would generate discord in the final state of a DQC1 algorithm. For example, consider the subgroup of the unitary group, $\mathcal{V}(d) \subset U(d)$, defined as $\mathcal{V}(d) = \{V^{\otimes n};\, V \in U(2)\}$ for $d = 2^n$. Writing V as

$$V = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \tag{5.30}$$

  for complex matrix elements $\alpha, \beta, \gamma, \delta$ satisfying $V^\dagger V = I$, the trace is equal to

$$\mathrm{Tr}(V^{\otimes n}) = \sum_{k=0}^{n} \binom{n}{k} \alpha^n \delta^{n-k}, \tag{5.31}$$

  which can be efficiently determined, requiring at most a polynomial number of queries. However, some of these unitaries in $\mathcal{V}(d)$ generate non-zero discord (provided they do not satisfy Eqn. (5.29)).

- The value of the GQD for DQC1-states is insensitive to phase errors in the final measurement. This is not the case in many NMR experiments: for instance, in the Jones polynomial experiments from Chapter 3, the phase was one of the major sources of error and had to be carefully tracked and calibrated. For DQC1 experiments, this phase insensitivity can eliminate much of the data post-processing. Currently, we must fit the real and imaginary parts of the spectrum very precisely in order to ensure we have the best approximation of the observables visible in that spectrum. When we are not worried about the phase, we are able to simply integrate the signal directly using the spectrometer software. Examples of this analysis are given in Section 5.3.

- The GQD of DQC1-states scale as $1/2^n$, indicating that the GQD decreases rapidly as the size of the completely mixed register grows. This is perhaps the most surprising property of the GQD for DQC1-states, as the quantum discord for an average DQC1-state does not decrease with the size of the system. In fact, the quantum discord for an average DQC1-state is independent of the size of the bottom register for large n. A previous numerical study [BPPC11] compared quantum discord and geometric quantum discord on two qubit states and they found that there was a strong correlation between the two quantities.

The qualitative similarities and differences for the QD and GQD of DQC1-states can be better investigated by generating plots for unitaries randomly drawn from the Haar measure for a small number of qubits and plotting the geometric discord. This is done in Figures 5.6 and 5.7 and can be compared with the plots for the QD in Figures 5.1 and 5.2, noting that the GQD plots are multiplied by 2^n on the vertical axis to assist the reader during comparison. We can see that aside from the $1/2^n$ dependence in the geometric discord, they both have a similar dependence on the polarization. In Figure 5.8 we plotted the average and standard deviation of the GQD (without scaling by 2^n) over the 500 numerically generated values on a log plot to illustrate the n dependence. This behaviour of the geometric discord suggests that it and the quantum discord are measuring different quantities in the case of DQC1-states.

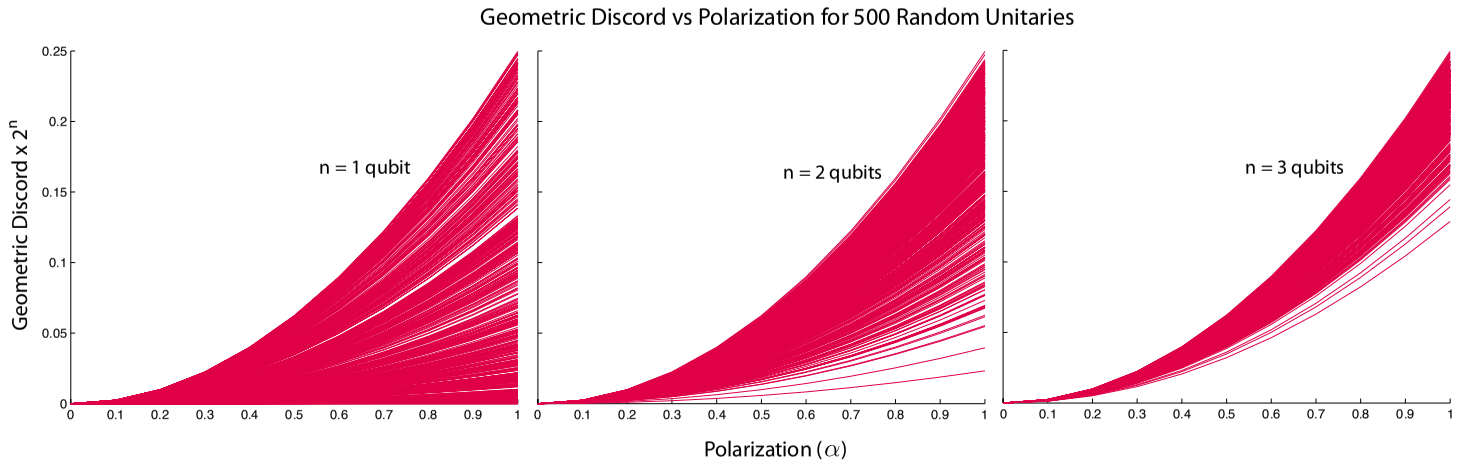

Figure 5.6: Geometric discord for randomly chosen DQC1-states with one, two, and three qubits in the bottom register. The states were created by choosing an 2^n-dimensional unitary at random from the Haar measure. The vertical axis for the geometric discord is multiplied by 2^n so that the plots for different n can be easily compared to those for the quantum discord.

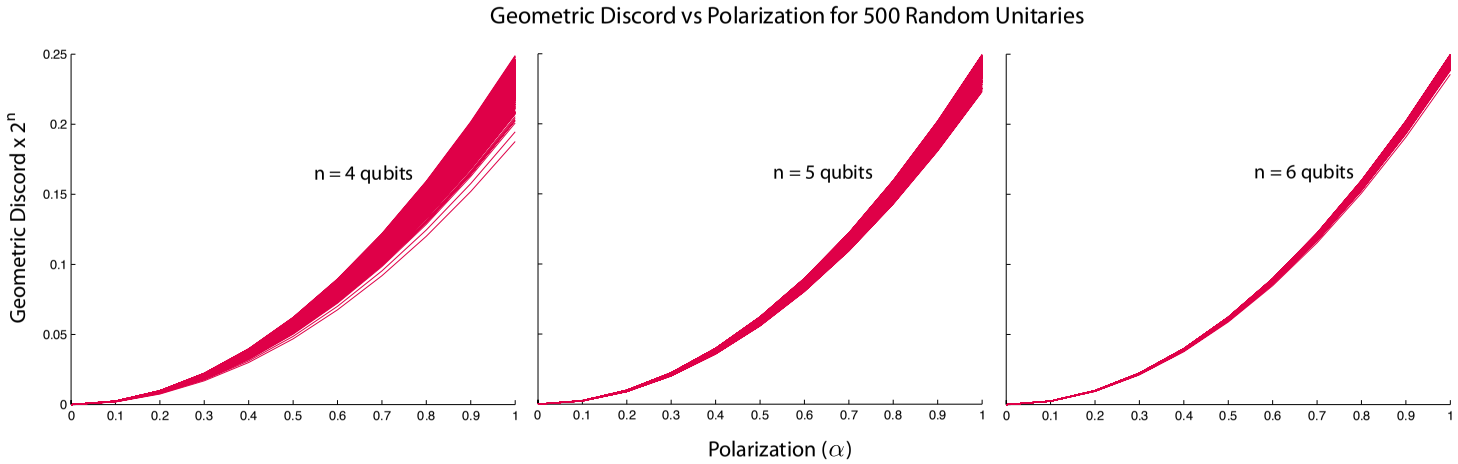

Figure 5.7: Figure for the geometric discord is the same as that in Figure 5.6 but for DQC1-states with four, five, and six qubits in the bottom register.

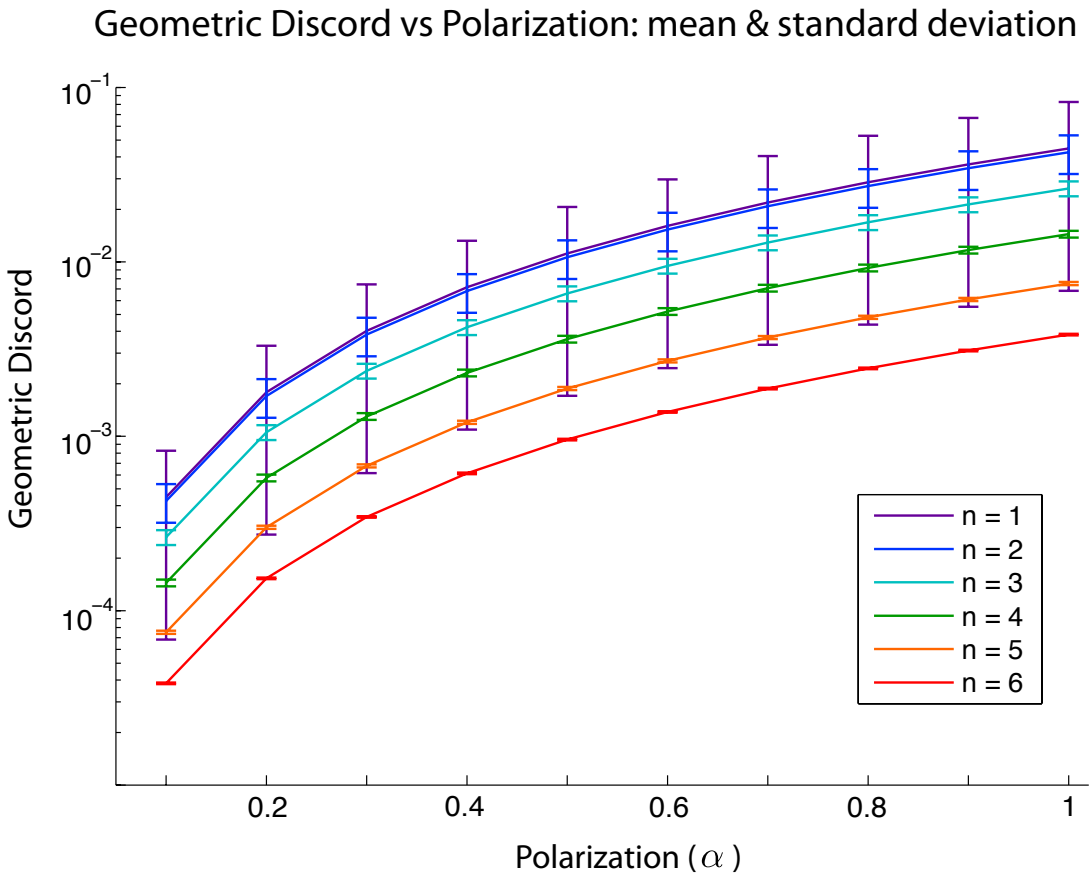

Figure 5.8: The mean geometric discord with standard deviation error bars for the data in Figures 5.6 and 5.7. Unlike the aforementioned plots, this data is not scaled by 2^n and is plotted with a logarithmic vertical axis, in order to illustrate the n-dependence.

- In order to more accurately compare the measures of GQD and QD for DQC1-states, we must look at the geometric discord for a 'typical' DQC1-state, as is done in Ref. [DSC08], where they found an expression for the average quantum discord to be

$$D_{avg}(\rho_{DQC1}) = 2 - H_2\left(\frac{1-\alpha}{2}\right) - \log(1+\sqrt{1-\alpha^2}) - (1-\sqrt{1-\alpha^2})\log e,$$

which is independent of the number of qubits for large n. Looking at our analytic expression for the geometric discord of a DQC1-state, we can easily find the average value for the geometric discord. A 'typical' instance of the DQC1 model is one where the unitary matrix is randomly distributed by the Haar measure, which implies that the eigenvalues are almost evenly spaced around the unit circle [Dia03]. Therefore, the trace is very small and can be approximated to zero (which is the same approximation made in Ref. [DSC08]). In doing this, the average geometric discord for a DQC1-state is approximated to

$$DG_{avg}(\rho_{DQC1}) = \frac{\alpha^2}{2^{n+2}}.$$

A graphical comparison of the two measures for the average quantum correlations in a DQC1-state is given in Figure 5.9. In order to plot the two measures of quantum correlations on the same scale, we have normalized the geometric discord first by a factor of two, since for a $2 \times d$ system, the maximum value for the geometric discord (for a maximally entangled state) is 0.5, whereas the maximum value of the quantum discord is one. We have also scaled the geometric discord by 2^n to make the plot independent of the number of qubits in the bottom register.

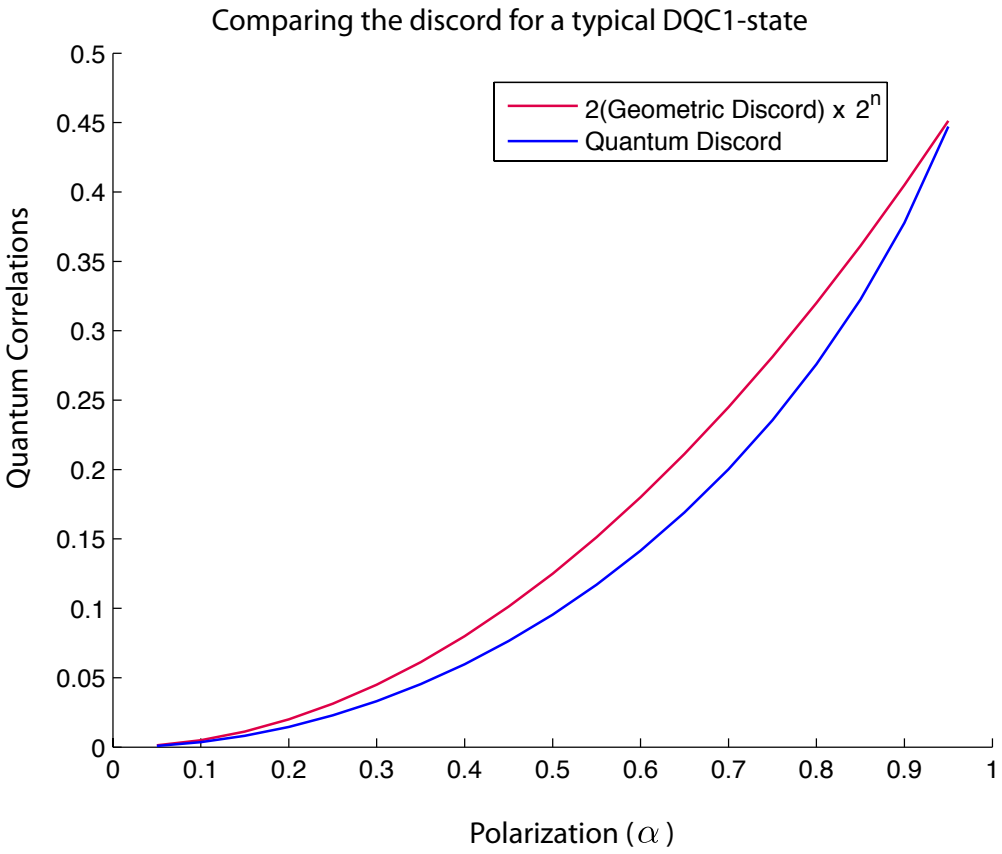

Figure 5.9: Plot comparing the quantum discord with the geometric quantum discord of 'typical' DQC1-states of n qubits. The approximation for the quantum discord (shown in blue) is valid for large n and has been shown to be a good approximation for $n > 5$ [DSC08]. The geometric discord is scaled by 2^{n+1} where a factor of 2 is for normalization and the 2^n factor is to remove the n-dependence of the GQD from the plot.

5.3 Experimental measurement of the geometric discord

In Section 5.2.2 we derived an analytical expression for the geometric quantum discord present in a DQC1 algorithm of arbitrary size. We also found that the expression is easily calculated using the DQC1 model. Recall that the GQD for a DQC1-state is

$$D_G(\rho_{DQC1}) = \left(\frac{\alpha}{2}\right)^2 \frac{1}{2^n}\left[1 - \tau_2\right],$$

where $\tau_2 = |\mathrm{Tr}(U^2)|/2^n$, n is the number of qubits in the bottom register, and α is the polarization of the top qubit.

In this section we experimentally measure the geometric quantum discord in an instance of the DQC1 model. In particular, we measure the GQD in the state that we detected quantum discord in Chapter 4. Recall that the unitary used is one of the unitaries used to approximate the Jones polynomial, and is of the form $U = \mathrm{diag}(a, a, b, 1, a, b, 1, 1)$, where $a = -(e^{-i3\pi/5})^4$ and $b = (e^{-i3\pi/5})^8$. The experiment is performed in liquid state NMR using four carbon-13 nuclei in trans-crotonic acid (nuclear structure, Hamiltonian information and the experimental procedure are found in Appendix A). The circuit diagram for this experiment is given in Fig 5.4, where we have the usual DQC1 circuit, followed by an additional implementation of the controlled-U. The result of the usual DQC1 measurements yield

$$|\langle\sigma_x\rangle + i\langle\sigma_y\rangle| = \frac{\alpha|\mathrm{Tr}(U^2)|}{2^n} = \alpha\,\tau_2. \tag{5.32}$$

Figure 5.10 shows the Hilbert-Schmidt distance between the DQC1-state of interest and the closest classical state, $g(a, \phi) = ||\rho - \chi||^2$ as a function of the measurement parameters a and ϕ. The top contour plot has the phase ϕ along the horizontal axis and a along the vertical. The third dimension of the contour plot (the depth) is $g(a, \phi)$ normalized by α^2. The bottom plot is a cross-section of the top one where $a_0 = 1/\sqrt{2}$, the horizontal axis is still the phase, and the vertical axis is $g(\frac{1}{\sqrt{2}}, \phi)$. The plots are the analytical values, with the experimental result indicated on the bottom plot. The error bars on the experimental value are propagated from the error in experimental uncertainties and the spectral fit.

Our results indicate that we have a GQD for this particular DQC1-state of

$$D_G = (0.0260 \pm 0.0004)\alpha^2, \tag{5.33}$$

which, for the value of $\alpha = 1.4 \times 10^{-5}$, the value of the quantum correlations is $D_G = (5.10 \pm 0.08) \times 10^{-12}$. The theoretical value is calculated to be $D_G^{th} = 0.02657\alpha^2$.

The experimental results given above are determined by integrating the fitted NMR spectrum. Generally this is the best method for extracting data, however, when we do not need the exact phase of the spectrum, we can integrate directly on the NMR spectrometer software[3]. In doing so, we receive the result $(0.0262 \pm 0.0001)\alpha^2$, and as expected, changing the phase of the spectrum does not change the result. The uncertainty reported is due to the signal-to-noise ratio. These calculations were performed very easily using the spectrometer software, and give a very good estimate of the result.

5.4 Analytical results for two-qubit DQC1

In Section 5.2 we found an analytical expression for the GQD of DQC1-states of any dimension. In this section, we look at the quantum discord based on mutual information and derive an analytical expression for the special case of two-qubit DQC1-states. The mathematical details given here provide reasonable detail so that each step can be followed from the previous with only a small amount of algebra in-between. Those purely interested in the results can find the major pieces summarized in Section 5.4.1 before we find the final analytical expression and discuss in Section 5.4.2.

Recall that the equation for the quantum discord of a bipartite state is given by

$$D(A:B) = S(\rho_A) - S(\rho_{AB}) + \min_{\{P_k\}} \sum_k p_k S(\rho_{B|k}). \tag{5.34}$$

The initial state of our system is taken to be $\rho_i = \left(\frac{1}{2}I + \frac{\alpha}{2}X\right) \otimes \frac{1}{2}I$, where I is the identity on two qubits. At the end of the computation, the final two-qubit state is

$$\rho_{AB} = \frac{1}{4}\begin{pmatrix} I & \alpha U^\dagger \\ \alpha U & I \end{pmatrix}, \tag{5.35}$$

with eigenvalues

$$\lambda_{AB} = \frac{1}{2^2}(1-\alpha, 1-\alpha, 1+\alpha, 1+\alpha). \tag{5.36}$$

[3]We use the Bruker software, TopSpin.

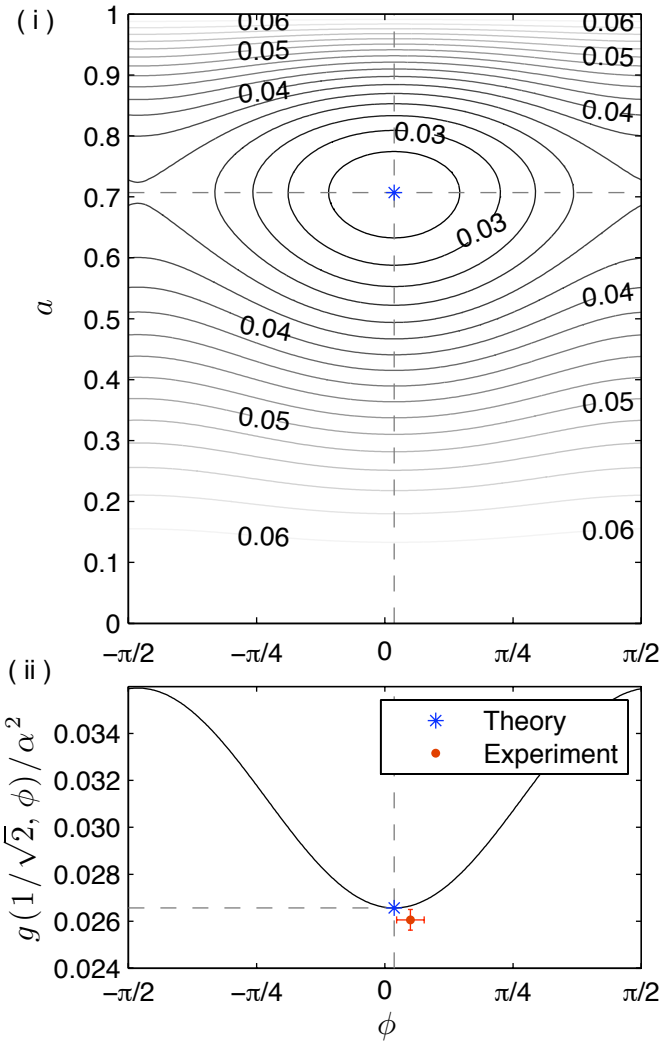

Figure 5.10: Shown are (i) the contour plot of the geometric distance, $g(a, \phi) = ||\rho_{DQC1} - \Pi^A(\rho_{DQC1})||^2$, normalized by α^2, as a function of the measurement parameters a and ϕ, for ρ_{DQC1} the output of the four-qubit DQC1 algorithm described in the text, and (ii) the geometric distance at the optimal measurement axis $a = a_0 = 1/\sqrt{2}$. The dashed lines indicate the parameters that correspond to the optimal measurement. The experimental data point for the geometric discord of ρ_{DQC1} is shown on plot (ii) with error bars propagated from experimental uncertainties and the spectral fit.

The joint entropy of the system is then given by

$$S(\rho_{AB}) = 1 + H_2\left(\frac{1-\alpha}{2}\right), \tag{5.37}$$

where $H_2(x) = x\log(x) + (1-x)\log(1-x)$ is the binary entropy. The reduced density matrix of system A is

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & \frac{\alpha}{2}\mathrm{Tr}(U^\dagger) \\ \frac{\alpha}{2}\mathrm{Tr}(U) & 1 \end{pmatrix}, \tag{5.38}$$

with eigenvalues

$$\lambda_A = \left(\frac{1-\alpha|\tau|}{2}, \frac{1+\alpha|\tau|}{2}\right), \tag{5.39}$$

where $\tau = \mathrm{Tr}(U)/2$, giving an entropy of

$$S(\rho_A) = H_2\left(\frac{1-\alpha|\tau|}{2}\right). \tag{5.40}$$

We now have two out of the three terms required to find the quantum discord from Eqn. (5.34). The last term is the minimization of the conditional entropy (Eqn. (2.48)) over all possible projective measurements. Let us start by defining our projectors, as in the previous case, to be $|\psi_\pm\rangle\langle\psi_\pm|$ where

$$|\psi_+\rangle = a|0\rangle + be^{i\phi}|1\rangle \tag{5.41}$$

$$|\psi_-\rangle = b|0\rangle - ae^{i\phi}|1\rangle, \tag{5.42}$$

are $\{a, b\} \in [0, 1]$ such that $a^2 + b^2 = 1$, and $\phi \in [0, 2\pi]$ are the parameters to be optimized over. The measurement operator acting on the two qubit system is then

$$|\psi_\pm\rangle\langle\psi_\pm| \otimes I = \begin{pmatrix} a^2 I & \pm abe^{-i\phi} I \\ \pm abe^{i\phi} I & b^2 I \end{pmatrix}, \tag{5.43}$$

and the state on system B after the measurement on system A yields $\{\pm\}$ is

$$\rho_{B|\pm} = \frac{1}{p_\pm}\mathrm{Tr}_A(|\psi_\pm\rangle\langle\psi_\pm| \otimes I\rho_{AB}) \tag{5.44}$$

$$= \frac{1}{4p_\pm}\Big((a^2+b^2)I \pm \alpha ab(e^{-i\phi}U + e^{i\phi}U^\dagger)\Big), \tag{5.45}$$

where p_+ and p_- are the probabilities of obtaining measurement outcome $(+)$ and $(-)$, respectively. Expressing U by its eigenvectors and eigenphases, $U = \sum_{j=1}^{2} e^{i\theta_j}|\theta_j\rangle\langle\theta_j|$ allows us to write

$$e^{-i\phi}U + e^{i\phi}U^\dagger = \sum_j e^{-i(\phi-\theta_j)}|\theta_j\rangle\langle\theta_j| + \sum_j e^{i(\phi-\theta_j)}|\theta_j\rangle\langle\theta_j| \tag{5.46}$$

$$= \sum_{j=1}^{2} 2\cos(\phi-\theta_j)|\theta_j\rangle\langle\theta_j|, \tag{5.47}$$

and simplify the state after measurement to

$$\rho_{B|\pm} = \frac{1}{p_\pm}\sum_{j=1}^{2}\left(\frac{1}{4} \pm \frac{\alpha}{2}ab\cos(\phi-\theta_j)\right)|\theta_j\rangle\langle\theta_j|, \tag{5.48}$$

where

$$p_\pm = \frac{1}{2} \pm \frac{\alpha}{2}ab\sum_j \cos(\phi-\theta_j). \tag{5.49}$$

Now we need to minimize $S(B|A) = \sum p_\pm S(\rho_{B|\pm})$. For simplicity, let us define the variable $x_j = \frac{\alpha}{2}ab\cos(\phi-\theta_j)$, so that

$$p_\pm = \frac{1}{2} \pm \sum x_j \text{ and} \tag{5.50}$$

$$\rho_{B|\pm} = \frac{1}{p_\pm}\sum(1/4 \pm x_j)|\theta_j\rangle\langle\theta_j|. \tag{5.51}$$

The eigenvalues of $\rho_{B|\pm}$ are

$$\lambda_+ = \left\{\frac{1}{p_+}\left(\frac{1}{4}+x_1\right), \frac{1}{p_+}\left(\frac{1}{4}+x_2\right)\right\} \text{ and } \lambda_- = \left\{\frac{1}{p_-}\left(\frac{1}{4}-x_1\right), \frac{1}{p_-}\left(\frac{1}{4}-x_2\right)\right\},$$

which will allow us to find the entropy. The conditional entropy that we need to minimize is composed of two terms:

$$\sum_\pm p_\pm S(\rho_{B|\pm}) = p_+ S(\rho_{B|+}) + p_- S(\rho_{B|-}), \tag{5.52}$$

let us look at each individually. The (+) term is

$$\begin{aligned} p_+ S(\rho_{B|+}) &= -p_+(\lambda_+^1 \log \lambda_+^1 + \lambda_+^2 \log \lambda_+^2) && (5.53)\\ &= -\left(\frac{1}{4}+x_1\right)\log\left(\frac{1/4+x_1}{p_+}\right) - \left(\frac{1}{4}+x_2\right)\log\left(\frac{1/4+x_2}{p_+}\right) && (5.54)\\ &= -\sum_j \left(\frac{1}{4}+x_j\right)\left(\log\left(\frac{1}{4}+x_j\right) - \log(p_+)\right). && (5.55) \end{aligned}$$

Similarly, the (−) term is

$$p_- S(\rho_{B|-}) = -\sum_j \left(\frac{1}{4}-x_j\right)\left(\log\left(\frac{1}{4}-x_j\right) - \log(p_-)\right), \tag{5.56}$$

and the sum, $S(B|A) = f(x) = \sum p_\pm S(\rho_{B|\pm})$, can be written as

$$f(x) = \sum_{j=1}^{2}\left[-\frac{1}{4}\log\left(\frac{(1/4+x_j)(1/4-x_j)}{p_+p_-}\right) - x_j \log\left(\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right)\right]. \tag{5.57}$$

We will perform the minimization by taking the first derivatives and setting them equal to zero: $\frac{df}{da} = 0$ and $\frac{df}{d\phi} = 0$. To keep the minimization process as streamlined as possible, we will find the total differential of $f(x)$, in terms of the variables x and $p_\pm$, after which, we perform a change of variables to a and ϕ. The details of the minimization are detailed below, but the confirmation that the results we find are a minimum is located in Appendix B.2. For simplicity, let us write Eqn. (5.57) as $f(x) = \sum_j (f_1(x_j) + f_2(x_j))$ and look at each term separately. The first term is written as,

$$\begin{aligned} df_1(x_j) = -\frac{\log_2(e)p_+p_-}{4(1/4+x_j)(1/4-x_j)}\Bigg[&\frac{\Big((1/4+x_j)(-dx_j) + (1/4-x_j)dx_j\Big)p_+p_-}{p_+^2p_-^2} && (5.58a)\\ &- \frac{(1/4+x_j)(1/4-x_j)\Big(p_-dp_+ + p_+dp_-\Big)}{p_+^2p_-^2}\Bigg]\\ = \frac{\log_2(e)x_jdx_j}{2(1/4+x_j)(1/4-x_j)} &+ \frac{\log_2(e)dp_+}{4p_+} + \frac{\log_2(e)dp_-}{4p_-}, && (5.58b) \end{aligned}$$

while the second term is

$$
\begin{aligned}
df_2(x_j) = &-dx_j \log\left(\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right) \\
&- \frac{x_j \log_2(e)(1/4-x_j)p_+}{(1/4+x_j)p_-}\left[\frac{\Big((1/4+x_j)dp_- + dx_j p_-\Big)(1/4-x_j)p_+}{(1/4-x_j)^2 p_+^2}\right. \qquad (5.59a)\\
&\qquad\left. - \frac{(1/4+x_j)p_-\Big(dp_+(1/4-x_j) - dx_j p_+\Big)}{(1/4-x_j)^2 p_+^2}\right] \\
= &-dx_j \log\left(\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right) + \log_2(e) x_j \left(\frac{dp_+}{p_+} - \frac{dp_-}{p_-}\right) \qquad (5.59b)\\
&- \frac{\log_2(e) x_j dx_j}{2(1/4+x_j)(1/4-x_j)}.
\end{aligned}
$$

Putting it all together,

$$
\begin{aligned}
df(x) = \sum_{i=1}^{2} &\left[-dx_j \log\left(\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right) - \log_2(e) x_j \left(\frac{dp_+}{p_+} - \frac{dp_-}{p_-}\right)\right] \qquad (5.60)\\
&+ \frac{\log_2(e)}{2}\left(\frac{dp_+}{p_+} + \frac{dp_-}{p_-}\right).
\end{aligned}
$$

Recall that $p_\pm = \frac{1}{2} + \sum x_j = \frac{1}{2} + x_1 + x_2$, so $dp_\pm = \pm \sum dx_j = \pm(dx_1 + dx_2)$. It is then possible to simplify the following terms:

$$
\begin{aligned}
\frac{dp_+}{p_+} + \frac{dp_-}{p_-} &= \frac{p_- dp_+ + p_+ dp_-}{p_+ p_-} \\
&= \frac{(1/2 - x_1 - x_2)(dx_1 + dx_2) + (-dx_1 - dx_2)(1/2 + x_1 + x_2)}{p_+ p_-} \\
&= \frac{-2(x_1 + x_2)(dx_1 + dx_2)}{p_+ p_-}, \qquad (5.61)
\end{aligned}
$$

and

$$
\frac{dp_+}{p_+} - \frac{dp_-}{p_-} = \frac{p_- dp_+ - p_+ dp_-}{p_+ p_-} = \frac{dx_1 + dx_2}{p_+ p_-}. \qquad (5.62)
$$

We can quickly see that the two terms in Eqn. (5.60) that contain $\log_2(e)$ cancel each other out, and we are left with the simplified expression

$$df(x) = -\sum_{i=1}^{2} dx_j \log\left(\frac{(1/4 + x_j)p_-}{(1/4 - x_j)p_+}\right). \tag{5.63}$$

Now that we have a simplified differential equation, we can determine what dx_j is in terms of the projective measurement variables a and ϕ:

$$\begin{aligned} x_j &= \frac{\alpha}{2} a(1-a^2)^{1/2}\cos(\phi - \theta_j) && (5.64)\\ dx_j &= \frac{\alpha}{2}\left((1-a^2)^{1/2} - \frac{a^2}{(1-a^2)^{1/2}}\right)\cos(\phi-\theta_j)da \\ &\quad -\frac{\alpha}{2}a(1-a^2)^{1/2}\sin(\phi-\theta_j)d\phi && (5.65)\\ &= \frac{\alpha}{2}\left(\frac{1-2a^2}{(1-a^2)^{1/2}}\right)\cos(\phi-\theta_j)da - \frac{\alpha}{2}a(1-a^2)^{1/2}\sin(\phi-\theta_j)d\phi. && (5.66) \end{aligned}$$

To minimize f, we take the partial differential equations to zero: $\frac{df}{da} = 0$ and $\frac{df}{d\phi} = 0$, and solve. The first equation takes the form

$$\frac{df}{da} = 0 = \frac{1-2a^2}{(1-a^2)^{1/2}} \sum_{j=1}^{2}\left(\cos(\phi-\theta_i)\log\left(\frac{(1/4+x_i)p_-}{(1/4-x_j)p_+}\right)\right), \tag{5.67}$$

giving a solution of $a_0 = 1/\sqrt{2} = b_0$ (which we can quickly find by looking at the term in front of the sum). The solution to the second equation is a little more difficult to see, but after substituting the value of a_0 found above, and dividing by the constants, we are left with

$$\frac{df}{d\phi} = 0 = \sin(\phi-\theta_1)\log\left(\frac{(1/4+x_1)p_-}{(1/4-x_1)p_+}\right) + \sin(\phi-\theta_2)\log\left(\frac{(1/4+x_2)p_-}{(1/4-x_2)p_+}\right). \tag{5.68}$$

With the ansatz that $p_+ = p_-$, the above equation can be simplified further, noting that under this assumption, $x_1 = -x_2$. Eqn. (5.68) is then reduced to

$$\begin{aligned} \frac{df}{d\phi} &= 0 = (\sin(\phi-\theta_1) - \sin(\phi-\theta_2))\log\left(\frac{1/4+x_1}{1/4-x_1}\right) && (5.69)\\ &\Rightarrow \sin(\phi-\theta_1) = \sin(\phi-\theta_2). && (5.70) \end{aligned}$$

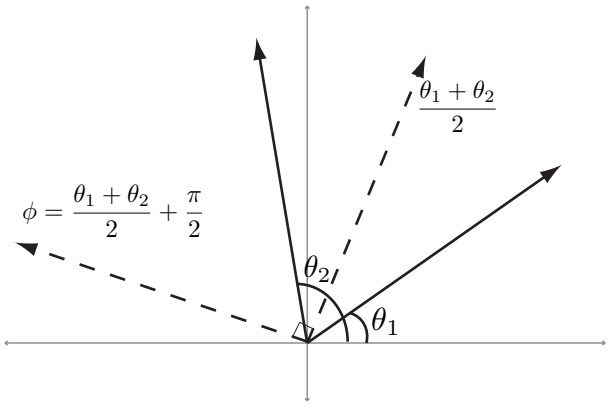

Figure 5.11: The two eigenphases for the unitary U are shown graphically with angles θ_1 and θ_2. The measurement that leads to the minimum value for the discord is parameterized by ϕ such that $\sin(\phi - \theta_1) = \sin(\phi - \theta_2)$. It can be seen that the cosines of $\phi - \theta_i$ will be equal when ϕ is in the middle of θ_1 and θ_2, which indicates that the sines will be equal when you add $n\pi/2$ to it, for integer values of n.

Eqn. (5.70) must hold if Eqn. (5.69) is satisfied and the ansatz holds true. The solution to this equation,

$$\phi_0 = \frac{\theta_1 + \theta_2}{2} + \frac{\pi}{2}, \tag{5.71}$$

is easiest to see graphically, as shown in Figure 5.11. To verify this result, let us look at both sides of Eqn. (5.70) and ensure they are equal. The left hand side becomes

$$\sin(\phi_0 - \theta_1) = \sin\left(\frac{\pi}{2} + \frac{\theta_2 - \theta_1}{2}\right) = \cos\left(\frac{\theta_2 - \theta_1}{2}\right), \tag{5.72}$$

while the right hand side is

$$\sin(\phi_0 - \theta_2) = \sin\left(\frac{\pi}{2} - \frac{\theta_2 - \theta_1}{2}\right) = \cos\left(-\frac{\theta_2 - \theta_1}{2}\right) = \cos\left(\frac{\theta_2 - \theta_1}{2}\right), \tag{5.73}$$

confirming $\phi_0 = \frac{\theta_1+\theta_2}{2} + \frac{\pi}{2}$ as a solution. Before stating the final results, we need to verify

that our ansatz is valid:

$$\begin{aligned}
p_+ = p_- = 1/2 \quad &\Rightarrow \quad x_1 = -x_2 \\
&\Rightarrow \quad \cos(\phi - \theta_1) = -\cos(\phi - \theta_2) \\
&\Rightarrow \quad \cos\left(\frac{\pi}{2} + \frac{\theta_2 - \theta_1}{2}\right) = -\cos\left(\frac{\pi}{2} - \frac{\theta_2 - \theta_1}{2}\right) \\
&\Rightarrow \quad -\sin\left(\frac{\theta_2 - \theta_1}{2}\right) = \sin\left(\frac{-(\theta_2 - \theta_1)}{2}\right) \\
&\Rightarrow \quad -\sin\left(\frac{\theta_2 - \theta_1}{2}\right) = -\sin\left(\frac{\theta_2 - \theta_1}{2}\right),
\end{aligned}$$

and since the final line is correct – our ansatz was valid. Therefore, the projective measurement parameters that minimize the discord are

$$a_0 = b_0 = \frac{1}{\sqrt{2}} \tag{5.74}$$

$$\phi_0 = \frac{\theta_1 + \theta_2}{2} + \frac{\pi}{2}. \tag{5.75}$$

5.4.1 Summarizing the results

Let us recap the important values before substituting everything into the equation for the discord. Recall that the quantum discord is given by $D(A:B) = S(\rho_A) - S(\rho_{AB}) + S(B|A)$, where $S(B|A) = \min_{\{P_k\}} \sum_k p_k S(\rho_{B|k})$. The first two terms in the discord are easy to compute, were calculated in Eqn. (5.40) and (5.37), and are

$$\begin{aligned}
S(\rho_A) &= H_2\left(\frac{1 - \alpha|\tau|}{2}\right) \\
S(\rho_{AB}) &= 1 + H_2\left(\frac{1 - \alpha}{2}\right),
\end{aligned}$$

where α is the polarization on the top register in the DQC1 model and $\tau = \mathrm{Tr}(U)/2^n = \mathrm{Tr}(U)/2$, for one qubit in the bottom register. The final term required an optimization over the projective measurements, $|\psi_\pm\rangle\langle\psi_\pm|$, where

$$\begin{aligned}
|\psi_+\rangle &= a|0\rangle + be^{i\phi}|1\rangle \\
|\psi_-\rangle &= b|0\rangle - ae^{i\phi}|1\rangle,
\end{aligned}$$

and we found the optimal values to be

$$\begin{aligned} a_0 &= b_0 = \frac{1}{\sqrt{2}} \\ \phi_0 &= \frac{\theta_1 + \theta_2}{2} + \frac{\pi}{2}, \end{aligned}$$

for a unitary that is characterized by its eigenphases: $U = \sum_{j=1}^{2} e^{i\theta_j} |\theta_j\rangle\langle\theta_j|$.

The conditional term $S(B|A)$ is

$$S(B|A) = \sum_{j=1}^{2} \left[-\frac{1}{4} \log \left(\frac{(1/4 + x_j)(1/4 - x_j)}{p_+ p_-} \right) - x_j \log \left(\frac{(1/4 + x_j)p_-}{(1/4 - x_j)p_+} \right) \right],$$

by substituting in that $x_1 = -x_2$ and $p_+ = p_- = 1/2$ we find

$$S(B|A) = -\frac{1}{2} \log \left(\frac{1}{4} - 4x_1^2 \right) - 2x_1 \log \left(\frac{1/4 + x_1}{1/4 - x_1} \right).$$

Recall that

$$x_1 = \frac{\alpha}{4} \cos(\phi_0 - \theta_1) = \frac{\alpha}{4} \cos \left(\frac{\pi}{2} + \frac{\theta_2 - \theta_1}{2} \right) = \frac{\alpha}{4} \sin \left(\frac{\theta_1 - \theta_2}{2} \right),$$

simplifying the conditional entropy term to

$$\begin{aligned} S(B|A) = 1 &- \frac{1}{2} \log \left(1 - \alpha^2 \sin^2 \left(\frac{\theta_1 - \theta_2}{2} \right) \right) \\ &- \frac{\alpha}{2} \sin \left(\frac{\theta_1 - \theta_2}{2} \right) \log \left(\frac{1 + \alpha \sin \left(\frac{\theta_1 - \theta_2}{2} \right)}{1 - \alpha \sin \left(\frac{\theta_1 - \theta_2}{2} \right)} \right). \end{aligned} \tag{5.76}$$

Putting Eqns. (5.40), (5.37), and (5.76) together, we find the analytical equation for the QD of a state at the conclusion of a two-qubit DQC1 algorithm to be

$$\begin{aligned} D(A:B) = H_2 &\left(\frac{1 - \alpha|\tau|}{2} \right) - H_2 \left(\frac{1 - \alpha}{2} \right) - \frac{1}{2} \log \left(1 - \alpha^2 \sin^2 \left(\frac{\theta_1 - \theta_2}{2} \right) \right) \\ &- \frac{\alpha}{2} \sin \left(\frac{\theta_1 - \theta_2}{2} \right) \log \left(\frac{1 + \alpha \sin \left(\frac{\theta_1 - \theta_2}{2} \right)}{1 - \alpha \sin \left(\frac{\theta_1 - \theta_2}{2} \right)} \right). \end{aligned} \tag{5.77}$$

5.4.2 Discussion

The most interesting property of the analytical expression found for quantum discord in the output state of a two-qubit DQC1 algorithm is that it only depends on the trace of the unitary performed – which is precisely the quantity measured in the DQC1 algorithm. While it is clear that the first two terms in Eqn. (5.77) depend only on the trace of the unitary, it is not as easy to see that the value of $\theta_1 - \theta_2$ is also dependent on the trace of the unitary. We outline this below, then rewrite the equation for the quantum discord in terms of measurable quantities from the DQC1 algorithm.

By writing $U = \sum_{j=1}^{2} e^{i\theta_j} |j\rangle\langle j|$, we can see that

$$\begin{aligned} \mathrm{Tr}(U) &= e^{i\theta_1} + e^{i\theta_2} && (5.78)\\ &= e^{i\theta_2}(e^{i(\theta_1-\theta_2)} + 1) && (5.79)\\ |\mathrm{Tr}(U)|^2 &= (e^{i(\theta_1-\theta_2)} + 1)(e^{-i(\theta_1-\theta_2)} + 1) && (5.80)\\ &= 2(1 + \cos(\theta_1 - \theta_2)). && (5.81) \end{aligned}$$

We can then rewrite Eqn. (5.81) into a term that can directly be substituted into Eqn. (5.77):

$$\begin{aligned} |\tau|^2 &= \frac{|\mathrm{Tr}(U)|^2}{4} && (5.82)\\ &= \frac{1 + \cos(\theta_1 - \theta_2)}{2} && (5.83)\\ &= \frac{2\cos^2\left(\frac{\theta_1-\theta_2}{2}\right)}{2} && (5.84)\\ &= 1 - \sin^2\left(\frac{\theta_1 - \theta_2}{2}\right) && (5.85)\\ \Rightarrow \sin\left(\frac{\theta_1 - \theta_2}{2}\right) &= \sqrt{1 - |\tau|^2} && (5.86) \end{aligned}$$

Let us rewrite the equation for the quantum discord in terms of τ:

$$\begin{aligned} D(A:B) = H_2\left(\frac{1-\alpha|\tau|}{2}\right) - H_2\left(\frac{1-\alpha}{2}\right) - \frac{1}{2}\log\left(1 - \alpha^2(1-|\tau|^2)\right) \\ - \frac{\alpha}{2}\sqrt{1-|\tau|^2}\log\left(\frac{1+\alpha\sqrt{1-|\tau|^2}}{1-\alpha\sqrt{1-|\tau|^2}}\right). \end{aligned} \quad (5.87)$$

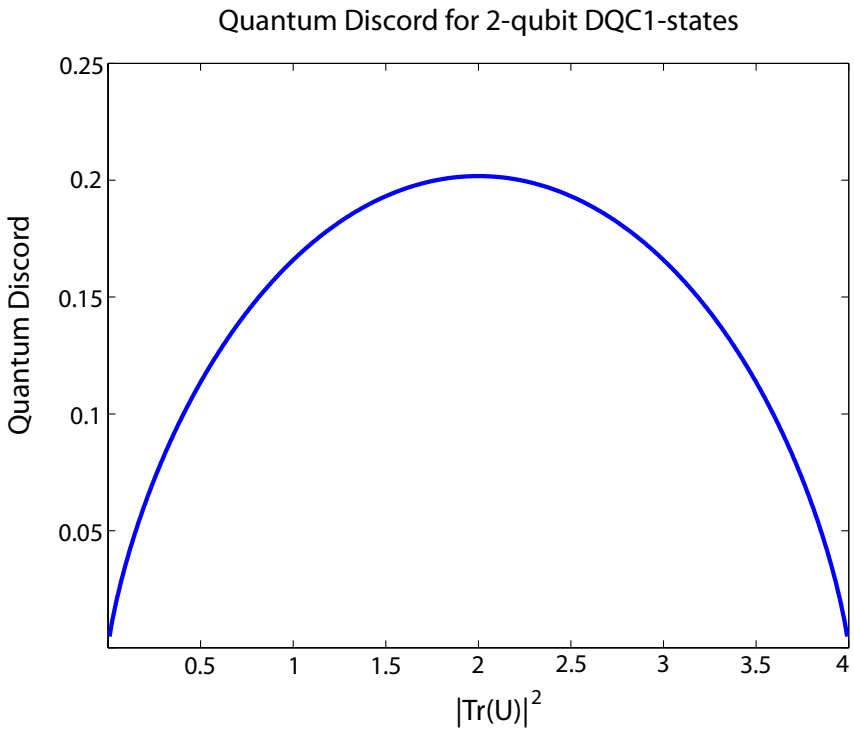

Figure 5.12: Graph of the quantum discord for states in the two-qubit DQC1 algorithm. The absolute value squared of the unitary in the DQC1 algorithm is plotted on the x-axis, with the corresponding quantum discord on the y-axis for a polarization of $\alpha = 1$.

Consequently, it is now evident that the quantum discord of a two-qubit DQC1-state only depends on the trace of the unitary. This allows us to calculate the QD for any two-qubit DQC1-state, which is graphically shown in Figure 5.12 for a polarization on the top qubit of one. We can see that the maximum value of the quantum discord is 0.2018 (which is considerably less than the QD of one for a maximally entangled state), which occurs when the absolute value of the trace squared is two. The minimum value of the QD is zero, and occurs when the absolute value of the trace of the unitary is zero or two. This is keeping with the result from Ref. [DVB10], which found that zero discord is found in DQC1 when the unitary can be written as a phase multiplied by a binary observable.

Interestingly, the quantum discord for two-qubit DQC1-states does not depend on the phase of the $\mathrm{Tr}(U)$, but only the absolute value. This is akin to the result for the geometric discord given in Section 5.2, and is beneficial for experimental measurements of the quantum discord for DQC1, as it eliminates a potential source of error.

The analysis in this section is only valid for two-qubit states; however, we have partial results extending our analysis to n qubits in the bottom register in Appendix C. The computation is much more difficult and we were unable to provide a complete analytical expression. However, if the parameters for the optimal measurement are able to be found, then it is possible to make a series approximation for the quantum discord, where each term can be evaluated using a DQC1 algorithm. More details are provided in the appendix.

5.4.3 Comparing QD and GQD for two-qubit DQC1 states

We now have analytical expression for both the quantum discord and the geometric quantum discord of two-qubit DQC1 states, which allows us to directly compare them. Let us look at the set of unitaries that give rise to the maximum QD and GQD. Note that we have already solved for the unitaries that give rise to minimum (zero) QD and GQD in Section 5.2.3. We found that $U = e^{i\xi/2}A$, where $A^2 = I$. Recall that the equation for GQD of any size DQC1-state is

$$D_G(\rho_{DQC1}) = \left(\frac{\alpha}{2}\right)^2 \frac{1}{2^n}\left[1 - \tau_2\right].$$

Analyzing what this means for the two-qubit case, we find that GQD (and hence, QD) is zero when

$$\begin{aligned}
\tau_2 = 1 \quad &\Rightarrow \quad \left|\mathrm{Tr}(U^2)\right| = 2 && (5.88)\\
&\Rightarrow \quad \left|e^{2i\theta_1} + e^{2i\theta_2}\right| = 2 && (5.89)\\
&\Rightarrow \quad \left|e^{2i\theta_1} + e^{2i\theta_2}\right|^2 = 4 && (5.90)\\
&\Rightarrow \quad 2 + 2\cos(2(\theta_1 - \theta_2)) = 4 && (5.91)\\
&\Rightarrow \quad 2(\theta_1 - \theta_2) = 2k\pi, \quad k \in \mathbb{Z} && (5.92)\\
&\Rightarrow \quad \theta_1 = \theta_2 + k\pi. && (5.93)
\end{aligned}$$

Performing the same analysis for when GQD is a maximum we find:

$$\begin{aligned}
\tau_2 = 0 \quad &\Rightarrow \quad \left|\mathrm{Tr}(U^2)\right| = 0 && (5.94)\\
&\Rightarrow \quad \left|e^{2i\theta_1} + e^{2i\theta_2}\right| = 0 && (5.95)\\
&\Rightarrow \quad \cos(2(\theta_1 - \theta_2)) = -1 && (5.96)\\
&\Rightarrow \quad 2(\theta_1 - \theta_2) = (2k+1)\pi, \quad k \in \mathbb{Z} && (5.97)\\
&\Rightarrow \quad \theta_1 = \theta_2 + (2k+1)\frac{\pi}{2}. && (5.98)
\end{aligned}$$

Let us now look at the unitaries that give rise to maximum QD. From Figure 5.12 we see that the maximum QD is when $|\mathrm{Tr}U|^2 = 2$. Therefore,

$$\begin{aligned}
|\mathrm{Tr}U|^2 &= 2 && (5.99)\\
\left|e^{2i\theta_1} + e^{2i\theta_2}\right|^2 &= 2 && (5.100)\\
2 + 2\cos(2(\theta_1 - \theta_2)) &= 2 && (5.101)\\
\cos(2(\theta_1 - \theta_2)) &= 0 && (5.102)\\
\theta_1 - \theta_2 &= (2k+1)\frac{\pi}{2}, \quad k \in \mathbb{Z} && (5.103)\\
\theta_1 &= \theta_2 + (2k+1)\frac{\pi}{2}, && (5.104)
\end{aligned}$$

which is the same result as for the GQD. To get a better idea of the QD and GQD as a function of the eigenphases θ_1 and θ_2, we plot the relationship in Figure 5.13. In order to accurately compare the two plots, we have plotted $2\times$ GQD to ensure that both the GQD and QD have a maximum value of 1. The plots have assumed the value of the polarization is $\alpha = 1$. To further compare, in Figure 5.14 we have taken a cross section of each plot from Figure 5.13, where $\theta_1 = -\theta_2$.

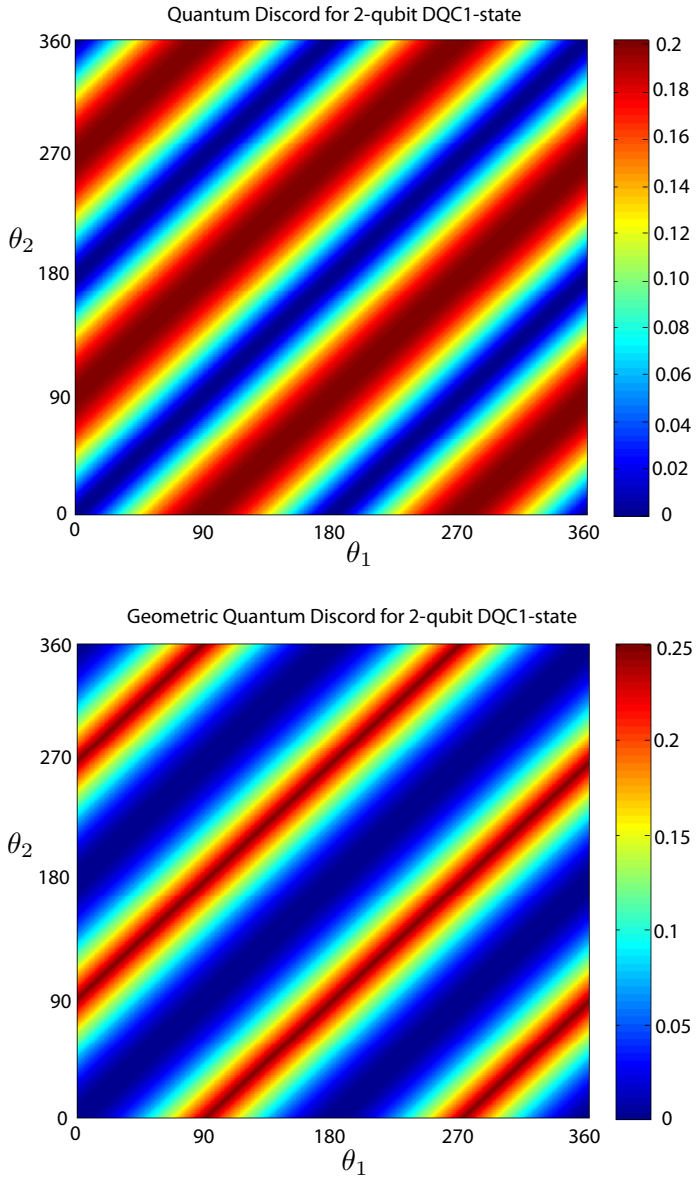

Figure 5.13: Plots of the quantum discord (top) and geometric quantum discord (bottom) for two-qubit DQC1-states. The QD and GQD are functions of the eigenphases θ_1 and θ_2 of the single-qubit unitaries. The GQD has been multiplied by a normalization factor of 2. These plots show that the two measures of non-classical correlations are a minimum and maximum for the same unitaries, but exhibit different values elsewhere. For instance, the GQD is closer to zero for a broader range of unitaries, while the QD has a larger value for more unitaries.

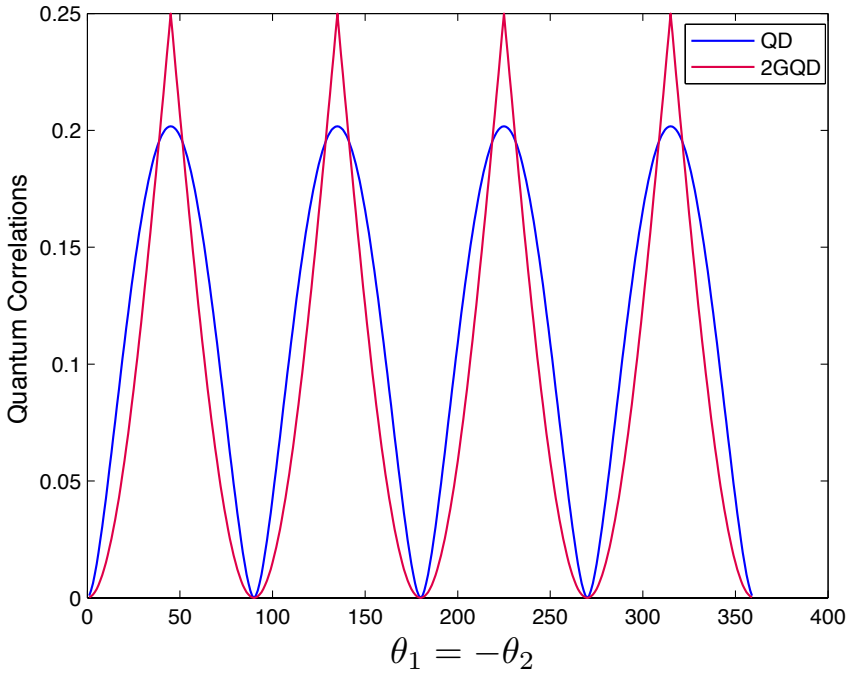

Figure 5.14: The quantum discord, shown in blue, and the geometric quantum discord (scaled by a factor of two), shown in red, for a cross section of two-qubit states. As can be seen in Figure 5.13, both measures for quantum correlations are periodic, and this plot captures all possible values. From this plot it is clear that both QD and GQD are zero for the same states and a maximum for the same states. This was mathematically shown in Eqns. (5.88)–(5.104).

5.5 Conclusion

In this chapter we looked at the quantity of non-classical correlations that exist in a DQC1-state by studying the measures of quantum discord and geometric quantum discord. We started by numerically investigating the quantum discord in DQC1-states for small numbers of qubits. We found that the spread, or standard deviation, of the quantum discord was much larger for a smaller number of qubits and decreased quickly as we added more qubits to the bottom register. It was discovered that while a 'typical' instance of a DQC1 algorithm was unlikely to deviate from the average value, this does not indicate the quantum discord of a given state will be near the average. This small spread in the quantum discord of DQC1-states for unitaries chosen from the Haar measure is a result of the concentration of measure and by looking at particular unitaries of experimental relevance, we were easily able to compute values for the quantum discord that lie between zero and the average.

Next, we were interested in finding an analytic expression for the non-classical correlations in a given DQC1-state without having to make any approximations or averages, that is simple to evaluate experimentally. In order to do this, we used the geometric quantum discord and were able to find closed-form expression that was easy to implement on a DQC1 quantum computer. In addition, we found that this measure only depends on the absolute value of the trace of the unitary squared and has a dependence on the number of qubits in the bottom register of $1/2^n$. This is in stark contrast to the quantum discord for a DQC1-state, for, while we do not have an exact analytic expression, numerical studies show that it does not have a similar n dependence. In Section 5.3, we experimentally measured the geometric discord in a four-qubit DQC1 experiment, performed in liquid state NMR, and successfully measured the geometric quantum discord to be $D_G = (5.10 \pm 0.08) \times 10^{-12}$.

Quantum discord has often been conjectured to be a potential resource for the apparent quantum advantage in the DQC1 model. However, this is questioned in recent work by Dakic, Vedral, and Brukner, where they found a set of unitaries that give rise to zero discord in the DQC1 model, yet it is unlikely that the trace of these unitaries can be efficiently calculated on a classical computer [DVB10]. On the other hand, we have found a set of unitaries that give rise to non-zero discord, yet their trace can be efficiently computed classically. Together, these findings suggest add to the suspicion that the apparent speedup exhibited by (the dynamics of) DQC1 is not necessarily captured by discord measures at the conclusion of the algorithm. In future work it would be very interesting to look at the

dynamics of discord measures throughout the DQC1 algorithm. In the NMR architecture, this could be done by looking at the discord at every time step of the numerically generated GRAPE pulses.

Finally, we switched from the measure of geometric quantum discord back to the quantum discord, and computed an analytic expression for the special case of two-qubits. We found that, similar to the geometric discord case, the final expression only depends on the absolute value of the trace of the unitary (only this time the unitary is not squared), indicating that it can be computed with a DQC1 quantum computer. With analytic expressions for both the quantum discord and geometric quantum discord for two-qubit DQC1-states, we were able to directly compare the values of the two measures, noting that they are both a maximum and minimum for the same unitaries, but the geometric discord has a sharper maximum peak and a smoother minimum peak while the quantum discord has the exact opposite.

While the research presented in this chapter is another step forward in understanding the correlations in the DQC1 model, there is more work that needs to be done. Specifically, we are interested in determining whether discord plays a role in the quantum advantage the DQC1 model offers. While we have looked at the final DQC1-state in this chapter, future work should consider the dynamics of the discord throughout the computation. In addition, future work should take a close look at different measures of quantum correlations and work to determine which measures provide the best picture for the quantum nature of quantum states.

Chapter 6

Conclusions and outlook

My interest in quantum information and computation has been motivated by the question of what makes a quantum computer *quantum*. This has lead me to study the DQC1 model of computation, which has the ability to outperform current classical methods, and yet, contains limited entanglement. This very intriguing model has been the focus of my research, and hence, this thesis. In the preceding chapters we have taken a closer (experimental) look at this model, its potential for solving problems of interest, and the quantum correlations it possesses.

This work started with a problem that completely encapsulates the power of the DQC1 model of computation. Approximating the Jones polynomial is a physically relevant problem with no known efficient classical algorithm, but can be solved on a quantum computer with very little or no entanglement. Implementing this problem in NMR was not only a proof-of-principle experiment, it pushed the limits of current control in liquid-state NMR as this experiment required extreme precision in order to distinguish different knots. Because of the accuracy required, we noticed issues with the metric used in our pulsefinding procedure. We found that two unitaries that are close using the gate fidelity figure of merit did not necessarily translate to the same level of accuracy when evaluating the trace. It is very possible that another figure of merit would be more appropriate for finding pulses used in the DQC1 algorithm.

Because of the lack of entanglement in an NMR implementation of DQC1 (such as the Jones polynomial experiment), the natural question that arises is whether or not there is any *quantum* computation taking place. Indeed, it is the spirit of this question that the

DQC1 model intended to provoke, and perhaps answer. We endeavoured to answer this question from an experimental point of view by looking to witness quantum correlations where there is no entanglement. It has been theoretically shown that on average, there is non-zero discord in the DQC1 model, however the value of the average quantum discord was found to decrease with the polarization. Because of the small polarization in liquid-state NMR, we set out to detect quantum discord in our experimental setup. Using a state-independent quantum discord witness, with only a few measurements we were able to detect non-classical correlations in a state where these correlations were calculated to be on the order of 10^{-11}. Interestingly, the value of the discord, which is dependent on the polarization, was not important when detecting quantum discord, provided we had a good signal-to-noise ratio. Witnessing this small amount of correlations begs the question of whether or not they are useful – an open question that is of much interest.

The final research presented in this thesis set out to quantify the quantum correlations in order to better understand if they are useful in the DQC1 model. Using the geometric quantum discord (GQD) as our measure of quantum correlations we were able to compose an experimentally measurable expression for correlations present in a DQC1-state. Measuring the GQD in these states is in the complexity class DQC1 and we provide experimental results for the GQD in the discord-detected NMR state mentioned above. A previous theoretical study looked at the average quantum discord in DQC1-states of higher dimension, and with our expression for the geometric quantum discord, we were able to compare the average correlations in higher-dimensional DQC1-states. Although there are some similarities between the two measures, one substantial difference is that the GQD scales with one over the dimension of the bottom register while the quantum discord is independent of this variable. Another interesting result is that we were able to find a group of unitary matrices that give rise to non-zero discord, and yet their trace can be efficiently calculated on a classical computer. Along with a previous result that found a set of unitaries that give zero discord but are unlikely to have a trace that can be efficient calculated, these results suggest that discord in the final DQC1-state may not be suitable to quantify the quantum advantage exhibited by the dynamics of the DQC1 algorithm.

The pursuit for a better understanding of the quantum nature of physical systems has led me, with the help of collaborators, to solve some very interesting questions. Along with this new-found information, we have uncovered many more questions than I would have thought to ask when this journey began. Only one thing is certain: the answers to these (and other) questions will undoubtedly expand our knowledge and lead to new discoveries.

APPENDICES

Appendix A

Four qubit liquid state NMR experimental parameters

Experiments in this thesis were performed using our workhorse liquid-state NMR four-qubit molecule, crotonic acid, pictured in Figure A.1. For use as a four-qubit quantum information processor the carbon nuclei, pictured in red, are synthesized to be carbon-13, while the hydrogen nuclei, pictured in blue, are decoupled using the WALTZ-16 and WALTZ-32 composite pulse sequences [SKF83]. The molecule is diluted in deuterated acetone and the ensemble of spin-1/2 molecules contains roughly 10^{20} spins. The experiments are implemented on a Bruker Avance 700 MHZ spectrometer. The parameters of the Hamiltonian at this field are given in Table A.1. Please note that the chemical shift terms are sensitive to the concentration and change slightly over a timescale of months.

The radio frequency (r.f.) pulses that implement the unitary transformations are numerically generated using the GRAPE algorithm [KRK$^+$05, RNL$^+$08] which starts from a random guess and is then iteratively improved through a gradient ascent search. The GRAPE pulses are optimized to produce a fidelity $|\mathrm{tr}(U_{goal}^{\dagger}U_{sim})|^2/d^2$, where d is the dimension of the Hilbert space of U_{goal}, of no less than 0.998. These pulses are designed to be robust to small inhomogeneities ($\pm 3\%$) in the r.f. control field.

In addition, the pulses are corrected for non-linearities in the pulse generation and transmission to the sample by measuring the r.f. signal at the position of the sample using a feedback loop and iteratively modifying the pulse accordingly [Rya08]. An example of a pulse (specifically, a controlled-σ_1^{-1} pulse from the Jones polynomial experiment in

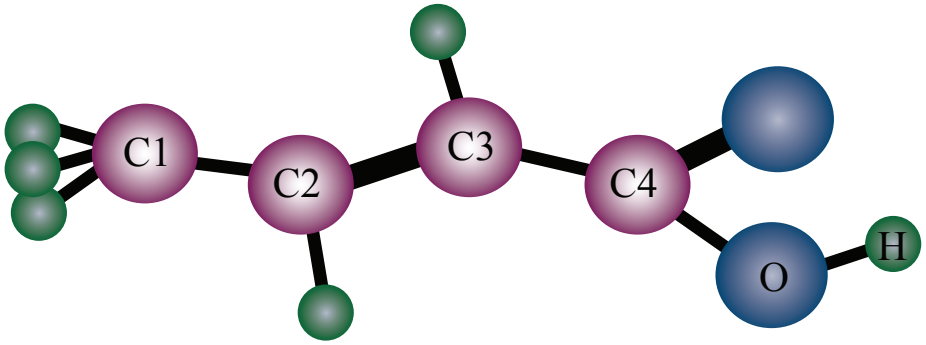

Figure A.1: Schematic of the chemical structure of crotonic acid. The red nuclei are carbon, the green are hydrogen and the blue nuclei are Oxygen. During the experiments, the protons are decoupled and the oxygen do not appear in the Hamiltonian because they have spin-0.

	C_1	C_2	C_3	C_4
C_1	2995			
C_2	41.6	25500		
C_3	1.5	69.6	21585	
C_4	7.0	1.2	72.3	29411

Table A.1: The parameters of the Hamiltonian given in Hz. The diagonal elements correspond to the chemical shifts ω_i with respect to the base frequency of carbon-13 (176.047829 MHz) with the Hamiltonian $\sum_i \pi\omega_i Z_i$. The off-diagonal elements represent the J-coupling constants J_{jk} with the Hamiltonian $\sum_{j<k} \frac{\pi}{2} J_{jk} Z_i Z_j$.

Chapter 3) can be seen in Figure A.2. This pulse has a length of 60ms and has been discretized into time-steps of 4μs. As can be seen in the figure, the final pulse ("Fix 6") is much closer to implementing the desired unitary than the first attempt. As mentioned above, the pulse is designed to have a fidelity of at least 0.998, however the implemented pulse fidelity is not this high. By simulating the implemented pulse we find that pulses of this length generally have a simulated fidelity of 0.99. Indeed, it is this fidelity that we use for estimating the implementation error in the Jones polynomial experiment.

A.1 Notes on pulsefinding for the DQC1 algorithm

In this section we will discuss the complications arising from pulsefinding the controlled unitary used in the DQC1 algorithm. Problems associated with this were first mentioned in Section 3.4. We will show that despite creating pulses with a fidelity of 0.998, the resulting measurement at the conclusion of the algorithm will not necessarily have as high fidelity. The fidelity function used to generate the pulses is called the gate fidelity and is written

$$F_g(U_{sim}, U_{id}) = \frac{|\mathrm{Tr}(U_{sim}U_{id}^\dagger)|^2}{d^2}, \tag{A.1}$$

where U_{sim} is the numerically generated pulse, U_{id} is the ideal pulse, and d is the dimension of the unitary.

Now, let us look at the types of pulses we create in the DQC1 algorithm. The pulses are controlled unitaries and the final measurement determines the trace of the unitary. So, although our pulse is designed to perform

$$cU = \begin{pmatrix} I_n & 0 \\ 0 & U_n \end{pmatrix}, \tag{A.2}$$

at the end of the day (or, more precisely, end of the algorithm), we are only measuring the trace of U_n. In the DQC1 algorithm, assuming perfect initial state preparation and perfect implementation of the Hadamard, the final state is (assuming unit polarization)

$$\begin{aligned} \rho_f &= cU\rho_i cU^\dagger & \text{(A.3)} \\ &= cU\,\frac{1}{2^{n+1}}\begin{pmatrix} I_n & \alpha I_n \\ \alpha I_n & I_n \end{pmatrix} cU^\dagger & \text{(A.4)} \\ &= \frac{1}{2^{n+1}}\begin{pmatrix} I_n & \alpha U_n^\dagger \\ \alpha U_n & I_n \end{pmatrix}, & \text{(A.5)} \end{aligned}$$

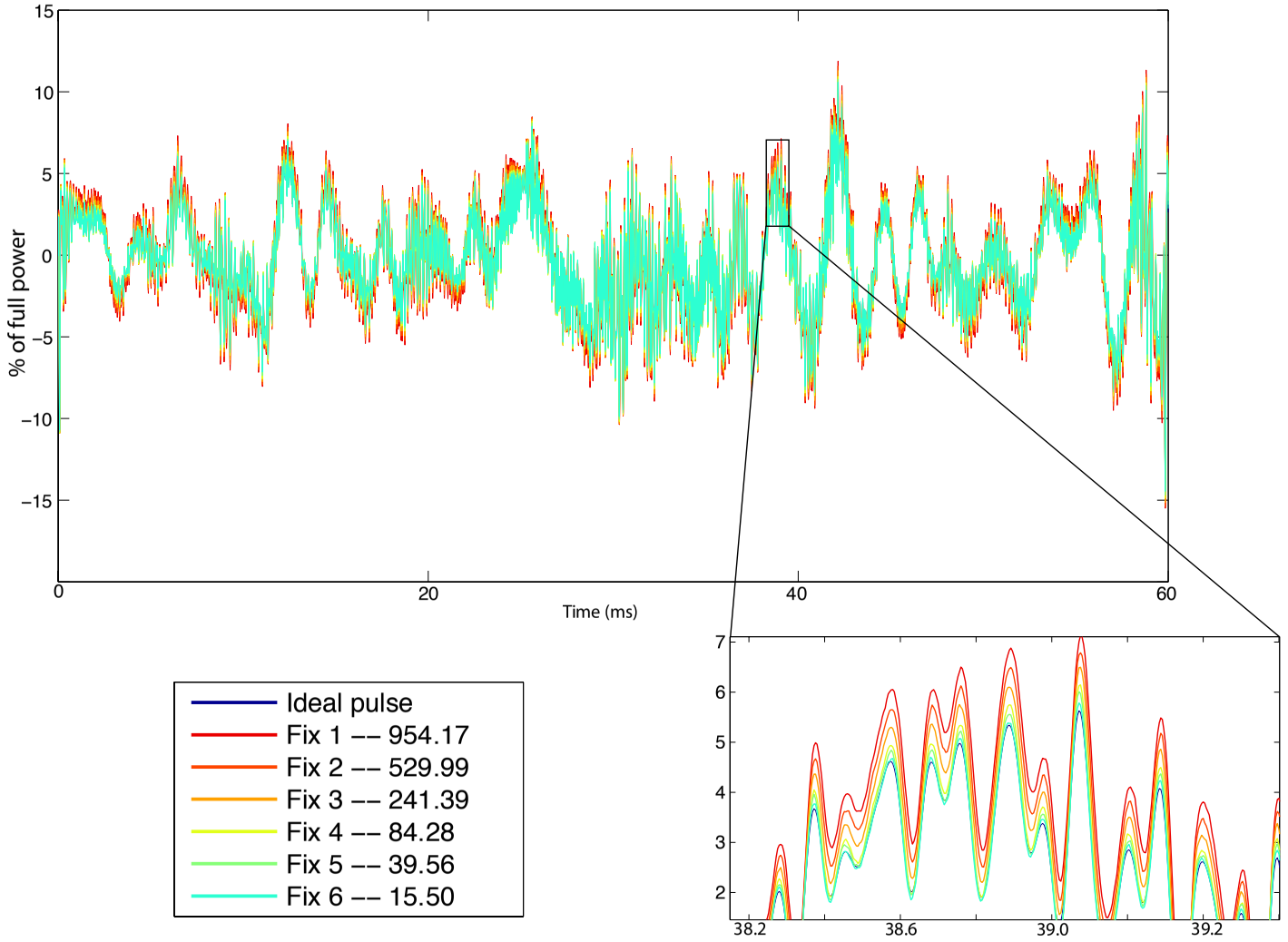

Figure A.2: Real part of the pulse generated by the GRAPE algorithm for implementing a controlled-σ_1^{-1} from the Jones polynomial experiment. The different colours indicate the iterative 'fixing' as measured by a feedback loop measuring the transmitted pulse at the location of the sample. The final pulse used in the experiment is labeled as "Fix 6" in the figure. Simulating this pulse (and others of the same duration) shows that it has a fidelity of approximately 0.99.

and the measured result is

$$M = \mathrm{Tr}\Big((\sigma_x \otimes I_n)\rho_f\Big) + i\mathrm{Tr}\Big((\sigma_y \otimes I_n)\rho_f\Big). \tag{A.6}$$

In order to determine how good our designed pulse is, we calculate the distance between M_{sim} and M_{id}:

$$D_{DQC1} = |M_{sim} - M_{id}|. \tag{A.7}$$

To see how well pulses of a particular gate fidelity perform in the DQC1 algorithm, we compared $F_g(U_{sim}, U_{id})$ to D_{DQC1}. The results are shown in Figure A.3. Each data point represents the mean D_{DQC1} for 300 simulated unitaries with that particular F_g. The error bars represent one standard deviation. Pulses numerically generated in this thesis were all found to have a gate fidelity of 0.998, which over a simulation of 300 different unitaries has $D_{DQC1} = 0.0051 \pm 0.0027$. The problematic part of this result is the very large error bars. This means that some pulses will perform much better in the DQC1 algorithm than others, despite having the same gate fidelity. In order to avoid this, in the Jones polynomial experiment from Chapter 3, we added a step to the pulsefinding procedure where we evaluate D_{DQC1} and only proceed with the pulses that have a D_{DQC1} value approximately equal to the desired fidelity.

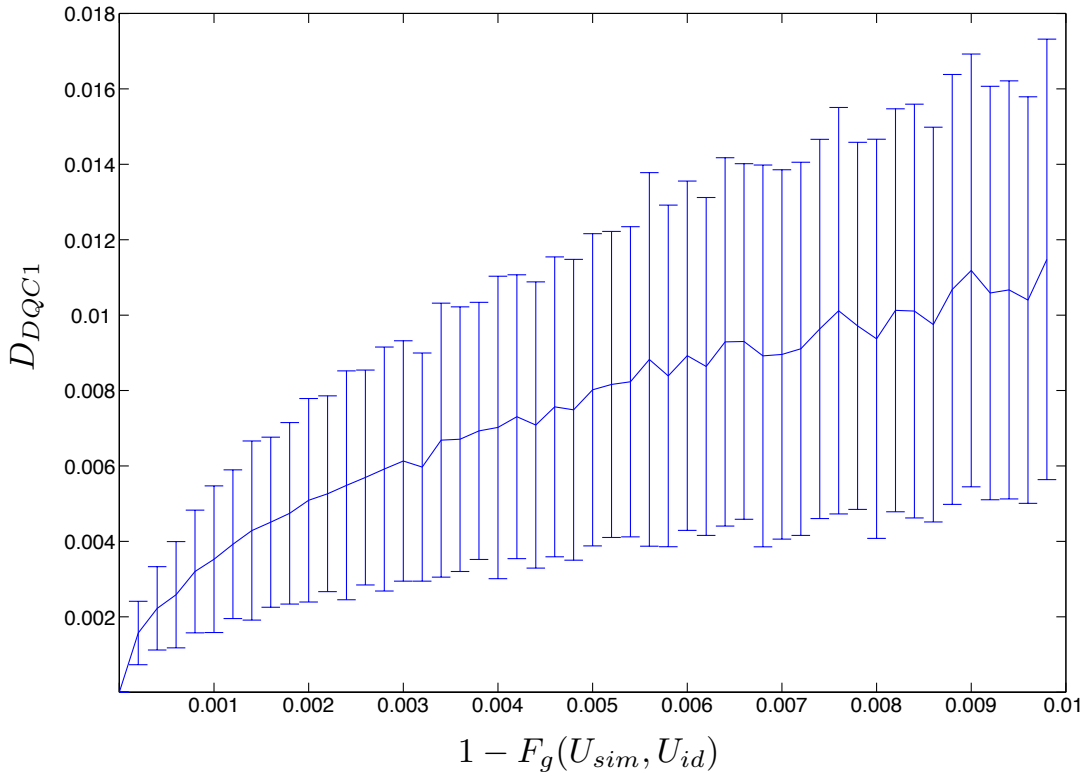

Figure A.3: Plot of the distance between the simulated and ideal final measurements (D_{DQC1}) in the DQC1 algorithm versus (one minus) the gate fidelity ($F_g(U_{sim}, U_{id})$) for the instance of the four qubit controlled-σ_1 unitary matrix (σ_1 is given in Eqn. (3.16)) used to approximate the Jones polynomial. Each data point is the mean value from 300 simulated pulses and the error bars give one standard deviation.

Appendix B

Analytical discord optimization

In this appendix we ensure that the values found during the optimization for the analytical calculation of the geometric discord (for n qubits) and the quantum discord (for 2 qubits) indeed correspond to minimums over their respective functions.

The possible extrema are found by taking the partial derivatives of the function in question. Solutions $a = x$ and $\phi = y$ to the following equations

$$\frac{\partial f}{\partial a} = 0 \tag{B.1}$$

$$\frac{\partial f}{\partial \phi} = 0 \tag{B.2}$$

are candidates for the optimal values of the function $f(a, \phi)$. In order to determine whether or not they correspond to a minimum, maximum or saddle point, we look to the Hessian matrix. The Hessian matrix is a square matrix of second-order derivatives of a multi-variable function. In our case, we have a function of variables a and ϕ that we would like to optimize. The Hessian matrix is then the two-by-two matrix:

$$H(f(x,y)) = \begin{pmatrix} f_{aa}(x,y) & f_{a\phi}(x,y) \\ f_{\phi a}(x,y) & f_{\phi\phi}(x,y) \end{pmatrix}, \tag{B.3}$$

where $f_{mn} = \frac{\partial^2 f}{\partial m \partial n}$. Then,

- if $|H(f(x,y))| > 0$ and $f_{aa}(x,y) > 0$, then (x,y) is a local minimum of f, or

- if $|H(f(x,y))| > 0$, and $f_{aa}(x,y) < 0$, then (x,y) is a local maximum of f, or
- if $|H(f(x,y))| < 0$, then (x,y) is a saddle point of f, and
- if $|H(f(x,y))| = 0$, then the test is inconclusive.

The notation $|H|$ indicates the determinant of matrix H. In order to ensure that the optima found are global, we also test the functions at the boundaries. Let's jump right into the optimization!

B.1 Optimization for the Geometric Quantum Discord

We start by performing the optimization for the geometric discord. The expression for the geometric discord before minimization is given in Eqn. (5.9) and looks like

$$D_G^A(\rho_{DQC1}) = \min_{\Pi^A} \left(\frac{1+\alpha^2}{2^{n+1}} - \frac{\alpha^2 a^2 b^2}{2^{2n+1}} \mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) - \frac{2\alpha^2 a^2 b^2 + 1}{2^{n+1}} \right).$$

In Section 5.2.2 we showed that the optimal values for the measurement are

$$a_0 = \frac{1}{\sqrt{2}} \rightarrow b_0 = \frac{1}{\sqrt{2}} \tag{B.4}$$

$$\phi_0 = \frac{1}{2}\tan^{-1}\left(\frac{\mathrm{Imag}(\mathrm{Tr}(U^2))}{\mathrm{Real}(\mathrm{Tr}(U^2))}\right). \tag{B.5}$$

In this appendix, we want to ensure that these values correspond to a minimum GQD. In order to do this, we compute the terms of the Hessian matrix:

$$f_{aa}(a,\phi) = \frac{\partial f}{\partial a}\left(\frac{2\alpha^2 a(1-2a^2)}{2^{2n+1}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) + \frac{4\alpha^2 a(1-2a^2)}{2^{n+1}}\right) \tag{B.6}$$

$$= \frac{\alpha^2}{2^{2n}}(1-6a^2)\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) + \frac{\alpha^2}{2^{n-1}}(1-6a^2). \tag{B.7}$$

For our value of ϕ, we can see that $\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) = 2|\mathrm{Tr}(U^2)|$, which is worked out in Eqns. (5.19)-(5.22). For convenience, we have rewritten the explanation here. Let us write $\mathrm{Tr}(U^2) = re^{i\eta}$, where $r = |\mathrm{Tr}(U^2)|$ and

$$\eta = \tan^{-1}\left(\frac{\mathrm{Im}[\mathrm{Tr}(U^2)]}{\mathrm{Re}[\mathrm{Tr}(U^2)]}\right) = 2\phi,$$

then

$$\begin{aligned}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) &= \left(e^{2i\phi}\mathrm{Tr}(U^{\dagger 2}) + e^{-2i\phi}\mathrm{Tr}(U^2)\right) \\ &= r\left(e^{i(2\phi-\eta)} + e^{-i(2\phi-\eta)}\right) \\ &= r(2) = 2|\mathrm{Tr}(U^2)|.\end{aligned}$$

Getting back to solving for f_{aa}, we continue from Eqn. (B.7), where defining $\tau = |\mathrm{Tr}(U^2)|/2^n$ and imputing $a = 1/\sqrt{2}$ leads to the simplification:

$$f_{aa} = \frac{\alpha^2}{2^n}(2\tau + 2)(-2) \tag{B.8}$$

$$= \frac{-\alpha^2}{2^{n-2}}(\tau + 1), \tag{B.9}$$

which is always negative since $\tau = |\mathrm{Tr}(U^2)|/2^n$ is positive.

Next, we look at the off-diagonal terms of the Hessian matrix, which both end up evaluating to zero at our solutions for a and ϕ:

$$\frac{\partial f}{\partial a \partial \phi} = \frac{\partial}{\partial a}\left(\frac{-\alpha^2 a^2(1-a^2)}{2^{2n-1}}\sum_j \sin(2(\phi - \theta_j))\right) \tag{B.10}$$

$$= \frac{-\alpha^2 2a(1-2a^2)}{2^{2n-1}}\sum_j \sin(2(\phi - \theta_j)) \tag{B.11}$$

$$= 0 \text{ for } a = \frac{1}{\sqrt{2}} \tag{B.12}$$

$$\frac{\partial f}{\partial \phi \partial a} = \frac{\partial}{\partial \phi}\left(\frac{\alpha^2 2a(1-2a^2)}{2^{2n+1}}\sum_j 2\cos(2(\phi - \theta_j)) + \frac{2\alpha^2 2a(1-2a^2)}{2^{n+1}}\right) \tag{B.13}$$

$$= \frac{\alpha^2 2a(1-2a^2)}{2^{n+1}}\sum_j -4\sin(2(\phi - \theta_j)) \tag{B.14}$$

$$= 0 \text{ for } a = \frac{1}{\sqrt{2}}. \tag{B.15}$$

The final term of the Hessian matrix is:

$$f_{\phi\phi}(a,\phi) = \frac{\partial}{\partial\phi}\left(\frac{-\alpha^2 a^2(1-a^2)}{2^{2n-1}}\sum_j \sin(2(\phi-\theta_j))\right) \tag{B.16}$$

$$= \frac{-\alpha^2 a^2(1-a^2)}{2^{2n-1}}\left(\sum_j 2\cos(2(\phi-\theta_j))\right) \tag{B.17}$$

$$= \frac{-\alpha^2}{2^{n+1}}\tau. \tag{B.18}$$

The final equality uses the same identity used to arrive at Eqn. (B.8), where we note that $\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) = \sum_j 2\cos(2(\phi-\theta_j))$.

The Hessian matrix is then

$$H(f(a,\phi)) = \begin{pmatrix} \frac{-\alpha^2}{2^n}(\tau+1) & 0 \\ 0 & \frac{-\alpha^2}{2^{n+1}}\tau \end{pmatrix}, \tag{B.19}$$

and has a determinant of

$$|H(f(a,\phi))| = \frac{\alpha^4}{2^{2n+1}}\tau(\tau+1) > 0. \tag{B.20}$$

Therefore, we have shown that the optimal values of

$$a_0 = \frac{1}{\sqrt{2}} \tag{B.21}$$

$$\phi_0 = \frac{1}{2}\arctan\left(\frac{\mathrm{Im}(\mathrm{Tr}(U^2))}{\mathrm{Re}(\mathrm{Tr}(U^2))}\right) \tag{B.22}$$

give rise to a local maximum for the function f which indicates that they lead to the local minimum geometric discord, as desired.

The only thing left to do is to show that we have a global maximum by evaluating the function at the boundary conditions. Note that ϕ does not have any boundaries as it is cyclic. Recall that the function is

$$f(a,\phi) = \frac{\alpha^2 a^2 b^2}{2^{2n+1}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) + \frac{2\alpha^2 a^2 b^2 + 1}{2^{n+1}}.$$

The boundaries of a are 0 and 1, which correspond to values for b of 1 and 0, respectively. Then it is easy to find the value of the function at these values:

$$f(0,\phi) = f(1,\phi) = \frac{1}{2^{n+1}}. \tag{B.23}$$

We need to compare this to the value of the function when $a = b = 1/\sqrt{2}$:

$$\begin{aligned} f(1/\sqrt{2},\phi) &= \frac{\alpha^2}{2^{2n+3}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) + \frac{2\alpha^2}{2^{n+3}} + \frac{1}{2^{n+1}} && \text{(B.24)} \\ &= \frac{1}{2^{n+1}}\left(\frac{\alpha^2}{2^{n+2}}\mathrm{Tr}(e^{2i\phi}U^{\dagger 2} + e^{-2i\phi}U^2) + \frac{\alpha^2}{2} + 1\right) && \text{(B.25)} \\ &= \frac{1}{2^{n+1}}\left(\frac{\alpha^2}{2^{n+2}}2|\mathrm{Tr}(U^2)| + \frac{\alpha^2}{2} + 1\right) && \text{(B.26)} \\ &= \frac{1}{2^{n+1}}\left(\frac{\alpha^2}{2}\tau + \frac{\alpha^2}{2} + 1\right) && \text{(B.27)} \\ &= \frac{1}{2^{n+1}} + \frac{\alpha^2}{2^{n+2}}(\tau + 1). && \text{(B.28)} \end{aligned}$$

Since $\tau > 0$, we have that $f(1/\sqrt{2},\phi) > f(0,\phi)$, and have shown that the boundaries are not a maximum. This indicates that the optimal values given in Eqns. (B.21) and (B.22) do indeed, give rise to the minimum geometric discord.

B.2 Optimization for the Quantum Discord

We will repeat the exact same procedure as for Section B.1, starting by reminding ourselves of the function we are minimizing, which is originally given in Eqn. (5.57):

$$f(a,\phi) = \sum_{j=1}^{2}\left[-\frac{1}{4}\log\left(\frac{(1/4+x_j)(1/4-x_j)}{p_+p_-}\right) - x_j\log\left(\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right)\right],$$

where $x_j = \frac{\alpha}{2}ab\cos(\phi-\theta_j)$, $p_+ = 1/2 + x_1 + x_2$, and $p_- = 1/2 - x_1 - x_2$. Also, remember that $b = \sqrt{1-a^2}$.

Looking back at the work in Section 5.4, we can see that the solutions we found for a and ϕ were the only solutions, so we only need to check the boundary conditions once we have ensured we indeed have a local minimum. Before diving into the mathematics, let us remind ourselves of the simplifications that occur for the solutions of $a = 1/\sqrt{2}$ and $\phi = \frac{\theta_1+\theta_2}{2} + \frac{\pi}{2}$. First, we have that $p_+ = p_- = 1/2$ and $x_1 = -x_2$. This also means that $\cos(\phi-\theta_1) = -\cos(\phi-\theta_2)$.

The first term we need to calculate for the Hessian is f_{aa}:

$$f_{aa} = \frac{\partial}{\partial a}\left(\frac{-\alpha}{2}\frac{1-2a^2}{(1-a^2)^{\frac{1}{2}}}\sum_j \cos(\phi-\theta_j)\log\left[\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right]\right) \tag{B.29a}$$

$$\begin{aligned} &= \frac{\partial}{\partial a}\left(\frac{-\alpha}{2}\frac{1-2a^2}{(1-a^2)^{\frac{1}{2}}}\right)\times\sum_j \cos(\phi-\theta_j)\log\left[\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right] \\ &\quad + \frac{-\alpha}{2}\frac{1-2a^2}{(1-a^2)^{\frac{1}{2}}}\frac{\partial}{\partial a}\left(\sum_j \cos(\phi-\theta_j)\log\left[\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right]\right). \end{aligned} \tag{B.29b}$$

From here we can see that the second line in Eqn. (B.29b) is equal to zero once we substitute in $a = 1/\sqrt{2}$.

$$\begin{aligned} f_{aa} &= \frac{-\alpha}{2}\left(\frac{(1-a^2)^{1/2}(-4a)-(1-2a^2)(1/2)(1-a^2)(-2a)}{1-a^2}\right) \\ &\quad\times\sum_j \cos(\phi-\theta_j)\log\left[\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right] \end{aligned} \tag{B.30a}$$

$$= \frac{-\alpha}{2}\left(\frac{(1-a^2)^{1/2}(-4a)}{1-a^2}\right)\sum_j \cos(\phi-\theta_j)\log\left[\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right] \tag{B.30b}$$

$$= 2\alpha\left(\cos(\phi-\theta_1)\log\left[\frac{(1/4+x_1)}{(1/4-x_1)}\right]+\cos(\phi-\theta_1)\log\left[\frac{(1/4+x_1)}{(1/4-x_1)}\right]\right) \tag{B.30c}$$

$$= 4\alpha\left(\cos(\phi-\theta_1)\log\left[\frac{(1/4+x_1)}{(1/4-x_1)}\right]\right) \tag{B.30d}$$

$$= 4\alpha\left(\cos(\phi-\theta_1)\log\left[\frac{(1+\alpha\cos(\phi-\theta_1))}{(1-\alpha\cos(\phi-\theta_1))}\right]\right) \tag{B.30e}$$

This value is always positive, regardless of the value of $\cos(\phi-\theta_1)$.

Now, let us look at the other diagonal term of the Hessian, $f_{\phi\phi}$:

$$f_{\phi\phi} = \frac{\partial}{\partial\phi}\left(\sum_j \frac{\alpha}{2} a(1-a^2)^{\frac{1}{2}} \sin(\phi-\theta_j) \log\left[\frac{(1/4+x_j)p_-}{(1/4-x_j)p_+}\right]\right) \tag{B.31a}$$

$$= \frac{\partial}{\partial\phi}\left(\frac{\alpha}{4}\left(\sin(\phi-\theta_1)-\sin(\phi-\theta_2)\right)\log\left[\frac{(1+\alpha\cos(\phi-\theta_1))}{(1-\alpha\cos(\phi-\theta_1))}\right]\right) \tag{B.31b}$$

$$\begin{aligned} = \frac{\alpha}{4}\frac{\partial}{\partial\phi}\left(\sin(\phi-\theta_1)-\sin(\phi-\theta_2)\right) \times \log\left[\frac{(1+\alpha\cos(\phi-\theta_1))}{(1-\alpha\cos(\phi-\theta_1))}\right] \\ + \frac{\alpha}{4}\left(\sin(\phi-\theta_1)-\sin(\phi-\theta_2)\right)\frac{\partial}{\partial\phi}\log\left[\frac{(1+\alpha\cos(\phi-\theta_1))}{(1-\alpha\cos(\phi-\theta_1))}\right]. \end{aligned} \tag{B.31c}$$

We know that $\sin(\phi-\theta_1) = \sin(\phi-\theta_2)$ (from Eqn. (5.70)), so the second line in Eqn. (B.31c) is zero and the expression simplifies to:

$$= \frac{\alpha}{4}\left(\cos(\phi-\theta_1)-\cos(\phi-\theta_2)\right)\log\left[\frac{(1+\alpha\cos(\phi-\theta_1))}{(1-\alpha\cos(\phi-\theta_1))}\right] \tag{B.32}$$

$$= \frac{\alpha}{2}\cos(\phi-\theta_1)\log\left[\frac{(1+\alpha\cos(\phi-\theta_1))}{(1-\alpha\cos(\phi-\theta_1))}\right]. \tag{B.33}$$

Therefore, $f_{\phi\phi}$ is positive for the same reasons that f_{aa} is positive in Eqn. (B.30e). The off-diagonal elements of the Hessian matrix are easily calculated to be zero, just as in the geometric discord case. This indicates that the determinant of the Hessian matrix is positive, as well as f_{aa}, and we have confirmed our solutions correspond to a local minimum.

Now, we just have to ensure the boundary conditions do not give rise to a smaller value for f. Just as in the geometric discord case, the value of ϕ is cyclic and has no boundary. We need to test for the case when $a = 0$, $b = 1$ and $a = 1$, $b = 0$. For both of these cases, we have that $x_j = 0$ and $p_+ = p_- = 1/2$. Therefore, the function is

$$f(0,\phi) = \sum_{j=0}^{1} -\frac{1}{4}\log\left(\frac{(1/4)(1/4)}{(1/2)(1/2)}\right) \tag{B.34}$$

$$= -\frac{1}{2}\log\left(\frac{1}{4}\right) \tag{B.35}$$

$$= 1. \tag{B.36}$$

We need to evaluate the function for $a = b = 1/\sqrt{2}$ to compare. We can start from the already simplified expression for f in Eqn. (5.76):

$$f(1/\sqrt{2},\phi) = 1 - \frac{1}{2}\log\left(1-\alpha^2\sin^2\left(\frac{\theta_1-\theta_2}{2}\right)\right) - \frac{\alpha}{2}\sin\left(\frac{\theta_1-\theta_2}{2}\right)\log\left(\frac{1+\alpha\sin\left(\frac{\theta_1-\theta_2}{2}\right)}{1-\alpha\sin\left(\frac{\theta_1-\theta_2}{2}\right)}\right).$$

Let $x = \frac{\theta_1-\theta_2}{2}$ for ease of notation, then we can simplify it as follows:

$$f(1/\sqrt{2},\phi) = 1 - \frac{1}{2}\log\left(1-\alpha^2\sin^2(x)\right) - \frac{\alpha}{2}\sin(x)\log\left(\frac{1+\alpha\sin(x)}{1-\alpha\sin(x)}\right) \tag{B.37a}$$

$$= 1 - \frac{1}{2}\log\left((1-\alpha\sin(x))(1+\alpha\sin(x))\right) - \frac{\alpha}{2}\sin(x)\log\left(\frac{1+\alpha\sin(x)}{1-\alpha\sin(x)}\right) \tag{B.37b}$$

$$= 1 - \frac{1}{2}\log(1-\alpha\sin(x)) - -\frac{1}{2}\log(1+\alpha\sin(x)) \tag{B.37c}$$
$$- \frac{\alpha}{2}\sin(x)\log(1+\alpha\sin(x)) - \frac{\alpha}{2}\sin(x)\log(1-\alpha\sin(x))$$

$$= 1 - \frac{1}{2}\Big[(1-\alpha\sin(x))\log(1-\alpha\sin(x)) + (1+\alpha\sin(x))\log(1+\alpha\sin(x))\Big]. \tag{B.37d}$$

The term in square brackets is always positive and is an element of $[0,1)$, implying that $f(1/\sqrt{2},\phi) < f(0,\phi)$. This concludes the demonstration that the optimal values $a_0 = 1/\sqrt{2}$ and $\phi_0 = \frac{\theta_1+\theta_2}{2} + \frac{\pi}{2}$, do indeed, correspond to a minimum in the quantum discord for two qubit DQC1-states.

Appendix C

Towards solving for the discord in n-qubit DQC1

In Section 5.4 we found an analytical expression for the quantum discord of a two-qubit DQC1 system. In this appendix we look at the extension to n qubits in the bottom register. The extension is straightforward until you reach the minimization, at which point we are unable to solve the system of equations that yield the optimal values of the measurement parameters. However, assuming that such a solution can be found, we find an expression for the quantum discord that can be measured using a sequence of DQC1 algorithms that does not grow as you add additional qubits. This will be explained in detail below.

The work in this appendix is most certainly a work in progress. A solution to the problems worked on here is certainly of interest and we hope one is found in the near future.

C.1 Quantum discord for an n-qubit DQC1-state

The two qubit case, while very interesting in that it only depends on the trace of the unitary, if of limited practical use. Therefore, we extended the analytical search for the discord to the n-qubit case. Our n-qubit state is initially $\rho_i = \left(\frac{1}{2}I + \frac{\alpha}{2}X\right) \otimes \frac{1}{2^n}I_n$, where n is the number of qubits in the bottom register. The state of the entire system at the

completion of the algorithm is

$$\rho_{AB} = \frac{1}{2^{n+1}} \begin{pmatrix} I^{\otimes n} & \alpha U^\dagger \\ \alpha U & I^{\otimes n} \end{pmatrix}, \tag{C.1}$$

with 2^n eigenvalues of the form $1/2^{n+1}(1-\alpha)$ and 2^n eigenvalues of the form $1/2^{n+1}(1+\alpha)$. The final reduced density matrix of system A is

$$\rho_A = \frac{1}{2} \begin{pmatrix} 1 & \frac{\alpha}{2^n}\mathrm{tr}(U^\dagger) \\ \frac{\alpha}{2^n}\mathrm{tr}(U) & 1 \end{pmatrix},$$

with eigenvalues

$$\lambda_A = \left(\frac{1-\alpha|\tau|}{2}, \frac{1+\alpha|\tau|}{2} \right),$$

where $\tau = \mathrm{Tr}(U)/2^n$. Therefore, the entropy of the full system is

$$S(\rho_{AB}) = n + H_2\left(\frac{1-\alpha}{2} \right), \tag{C.2}$$

and the entropy of the reduced system A is

$$S(\rho_A) = H_2\left(\frac{1-\alpha|\tau|}{2} \right). \tag{C.3}$$

These two entropy values are two of the three terms in Eqn. (5.34) for calculating the quantum discord. Now, we must perform the optimization over all projective measurement operators. To do so we follow the same procedure that was performed in the two qubit case, so we will be less explicit with the mathematical details in this section. The measurement is parameterized in the exact same way as given in Eqns. (5.41) and (5.42). The state on system B after measurement is taken directly from Eqn. (5.45) and we write the n-qubit unitary in terms of its eigenvectors and eigenphases as

$$U = \sum_{j=1}^{2^n} e^{i\theta_j} |\theta_j\rangle\langle\theta_j|, \tag{C.4}$$

simplifying the state

$$\begin{aligned}\rho_{B|\pm} &= \frac{1}{2^{n+1}p_\pm}(I \pm \alpha ab(e^{-i\phi}U + e^{i\phi}U^\dagger)) \\ &= \frac{1}{2^{n+1}p_\pm}(I \pm 2\alpha ab\sum_j \cos(\phi-\theta_j)|\theta_j\rangle\langle\theta_j|) \\ &= \frac{1}{p_\pm}\sum_{j=1}^{2^n}\left(\frac{1}{2^{n+1}} \pm \frac{\alpha ab}{2^n}\cos(\phi-\theta_j)\right)|\theta_j\rangle\langle\theta_j|. \end{aligned} \tag{C.5}$$

The probability of measuring the different outcomes is directly extended to n-qubits from Eqn. (5.49) to

$$p_\pm = \frac{1}{2} \pm \frac{\alpha ab}{2^n}\sum_j \cos(\phi-\theta_j). \tag{C.6}$$

Just as in the two-qubit case, let us define

$$x_j = \frac{\alpha ab}{2^n}\cos(\phi-\theta_j),$$

simplifying the above equations to

$$\rho_{B|\pm} = \frac{1}{p_\pm}\sum_{j=1}^{2^n}\left(\frac{1}{2^{n+1}} \pm x_j\right)|\theta_j\rangle\langle\theta_j|,$$

where

$$p_\pm = \frac{1}{2} \pm \sum_j x_j.$$

Then the conditional entropy term can be written as $S(B|A) = f(x) = \sum p_\pm S(\rho_{B|\pm})$, just as it was in Eqn. (5.57) with the sum extended,

$$f(x) = -\sum_{j=1}^{2^n}\left(-\frac{1}{2^{n+1}}\log\left(\frac{(\frac{1}{2^{n+1}}+x_j)(\frac{1}{2^{n+1}}-x_j)}{p_+p_-}\right) - x_j\log\left(\frac{(\frac{1}{2^{n+1}}+x_j)p_-}{(\frac{1}{2^{n+1}}-x_j)p_+}\right)\right),$$

and similarly for the differential

$$\begin{aligned} df(x) = \sum_{i=1}^{2^n}&\left[-dx_j\log\left(\frac{(\frac{1}{2^{n+1}}+x_j)p_-}{(\frac{1}{2^{n+1}}-x_j)p_+}\right) - \log_2(e)x_j\left(\frac{dp_+}{p_+} - \frac{dp_-}{p_-}\right)\right] \\ &+ \frac{\log_2(e)}{2}\left(\frac{dp_+}{p_+} + \frac{dp_-}{p_-}\right). \end{aligned} \tag{C.7}$$

By manipulating the terms containing $\log_2(e)$, we can see that they cancel (shown in detail in Section 5.4), and the differential reduces to

$$df(x) = \sum_{i=1}^{2^n} -dx_j \log\left(\frac{(\frac{1}{2^{n+1}} + x_j)p_-}{(\frac{1}{2^{n+1}} - x_j)p_+}\right).$$

By converting the parameters to those we want to optimize over,

$$\begin{aligned} x_j &= \frac{\alpha a(1-a^2)^{1/2}}{2^n}\cos(\phi - \theta_j) \\ dx_j &= \frac{\alpha}{2^n}\left(\frac{1-2a^2}{(1-a^2)^{1/2}}\right)\cos(\phi-\theta_j)da - \frac{\alpha}{2^n}a(1-a^2)^{1/2}\sin(\phi-\theta_j)d\phi, \end{aligned}$$

the equations we must satisfy in order to find a minimum are:

$$\frac{df}{da} = 0 = \frac{1-2a^2}{(1-a^2)^{1/2}}\sum_{j=1}^{2^n}\left(\cos(\phi-\theta_i)\log\left(\frac{(\frac{1}{2^{n+1}} + x_i)p_-}{(\frac{1}{2^{n+1}} - x_j)p_+}\right)\right), \tag{C.8}$$

$$\frac{df}{d\phi} = 0 = \sum_{j=1}^{2^n}\sin(\phi-\theta_j)\log\left(\frac{(\frac{1}{2^{n+1}} + x_j)p_-}{(\frac{1}{2^{n+1}} - x_j)p_+}\right). \tag{C.9}$$

Equation C.8 is satisfied when $a = b = 1/\sqrt{2}$, just as in the two-qubit case. However, Eqn. (C.9) is much more tricky. Since the probabilities $p_\pm$ are much more complex in the n-qubit case we are not able to assume that they are equal. This leaves us with the following complex equation to solve:

$$0 = \sum_{j=1}^{2^n}\sin(\phi-\theta_j)\log\left(\frac{(1+\alpha\cos(\phi-\theta_j))p_-}{(1-\alpha\cos(\phi-\theta_j))p_+}\right).$$

While we were not able to solve for ϕ from this equation, we continued with the analysis of the QD once a value of ϕ has been determined. This is detailed in the next section.

C.2 Experimentally determinable approximation for the discord of a $2 \times d$ DQC1-state

Although we have not yet determined the value of ϕ, we will proceed with the calculation for the quantum discord in an effort to gain insight and answer a few questions. One question

of interest is whether or not the quantum discord for DQC1-states can be experimentally determined. As we will see, they can be approximated on a DQC1 quantum information processor, provided the optimal value of ϕ is known.

Recall that the equation for the discord of a bipartite quantum state is given by $D(A:B) = S(\rho_A) - S(\rho_{AB}) + S(B|A)$. For $2 \times d$ DQC1 system, the first two terms are well known and given in Eqns. (C.3) and (C.2). These terms are easily evaluated provided the value of the polarization α is known and you can experimentally run the DQC1 algorithm to determine the trace of the unitary used. The final term is a little more complicated, but we show below how to formulate it in terms of quantities that can be experimentally determined, provided ϕ has been determined.

The conditional entropy term is

$$S(B|A) = -\sum_{j=1}^{2^n} \left(-\frac{1}{2^{n+1}} \log \left(\frac{(\frac{1}{2^{n+1}} + x_j)(\frac{1}{2^{n+1}} - x_j)}{p_+ p_-} \right) - x_j \log \left(\frac{(\frac{1}{2^{n+1}} + x_j)p_-}{(\frac{1}{2^{n+1}} - x_j)p_+} \right) \right),$$

where $x_j = \frac{\alpha}{2^{n+1}} \cos(\phi - \theta_j)$, $p_\pm = \frac{1}{2} \pm \sum_j x_j$. By defining $w_j = \alpha \cos(\phi - \theta_j)$, we can simplify $S(B|A)$:

$$\begin{aligned} S(B|A) &= \sum_{j=1}^{2^n} \left(-\frac{1}{2^{n+1}} \log \left(\frac{1}{2^{(n+1)^2}} \frac{(1+w_j)(1-w_j)}{p_+ p_-} \right) - \frac{w_j}{2^{n+1}} \log \left(\frac{(1+w_j)p_-}{(1-w_j)p_+} \right) \right) \\ &= \sum_{j=1}^{2^n} \frac{\log(2^{2n+1})}{2^{n+1}} - \frac{1}{2^{n+1}} \sum_{j=1}^{2^n} (\log(1+w_j) + \log(1-w_j) + w_j \log(1+w_j) \\ &\qquad - w_j \log(1-w_j) - \log p_+ - \log p_- + w_j \log p_- - w_j \log p_+) \\ &= n+1 - \frac{1}{2^{n+1}} \sum_{j=1}^{2^n} ((1+w_j)\log(1+w_j) + (1-w_j)\log(1-w_j)) + p_+ \log p_+ + p_- \log p_- \end{aligned}$$

The terms that contain the logarithm cannot be observed in a DQC1 experiment – so let us try to manipulate them into a better form.

First, note that the series expansion for $\log(1+x)$ and $\log(1-x)$ are

$$\log(1+x) = \sum_n^\infty \frac{(-1)^{n+1}}{n} x^n, \text{ and} \tag{C.10a}$$

$$\log(1+x) = \sum_n^\infty \frac{-1}{n} x^n, \tag{C.10b}$$

leading to

$$(1+x)\log(1+x) = \sum_n^\infty \left(\frac{(-1)^{n+1}}{n} x^n + \frac{(-1)^{n+1}}{n} x^{n+1} \right), \text{ and} \tag{C.11a}$$

$$(1-x)\log(1-x) = \sum_n^\infty \left(\frac{-1}{n} x^n + \frac{1}{n} x^{n+1} \right). \tag{C.11b}$$

Noticing that when summed, Eqns. (C.11a) and (C.11b) reduce to a sum over even numbers

$$(1+x)\log(1+x) + (1-x)\log(1-x) = 2 \sum_{neven} \frac{1}{n(n-1)} x^n, \tag{C.12}$$

which allows us to write the conditional entropy term as

$$S(B|A) = n + 1 + p_+ \log p_+ + p_- \log p_- - \frac{1}{2^{n+1}} \sum_{j=1}^{2^n} \sum_{keven}^\infty \frac{\alpha^k}{k(k-1)} \cos^k(\phi - \theta_j). \tag{C.13}$$

We are then able to break this down one step further, so that the powers of cosines turn into cosines of multiple angles, using the following relation for even k:

$$\cos^k(x) = \frac{1}{2^k} \binom{k}{\frac{k}{2}} + \frac{2}{2^k} \sum_{l=0}^{k/2-1} \binom{k}{l} \cos\left((k-2l)x\right).$$

Therefore, the final version of the conditional entropy is of the form

$$\begin{aligned} S(B|A) = n + 1 + p_+ \log p_+ + p_- \log p_- &- \frac{1}{2^{n+1}} \sum_{j=1}^{2^n} \sum_{keven}^\infty \frac{\alpha^k}{k(k-1)} \frac{1}{2^k} \binom{k}{\frac{k}{2}} \\ &- \frac{1}{2^{n+1}} \sum_{j=1}^{2^n} \sum_{k\ even}^\infty \frac{\alpha^k}{k(k-1)} \frac{2}{2^k} \sum_{l=0}^{k/2-1} \binom{k}{l} \cos\left((k-2l)(\phi - \theta_j)\right). \end{aligned} \tag{C.14}$$

While this term looks complicated, if we know that value of ϕ, we are able to measure

$$\sum_j \cos(m(\phi - \theta_j)) = \frac{2^n \langle \sigma_x \rangle_{r \times m}}{\alpha}, \tag{C.15}$$

where $\langle \sigma_x \rangle_{r \times m}$ is the expectation value of σ_x, measured after a DQC1 algorithm where there has been a rotation

$$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}, \tag{C.16}$$

directly before the controlled-unitary, applied back-to-back m times. Thus, all terms in Eqn. (C.14) can be determined experimentally using a DQC1 quantum information processor. Because the series converges, it is possible to approximate the value of the quantum discord experimentally, with a number of experiments that independent of the size of the system.

For an example of how the series converges for three qubits, the plot in Figure C.1 shows the approximation of the quantum discord using Eqn. (C.14) with a maximum k value on the horizontal axis. The unitary was randomly chosen from the Haar measure.

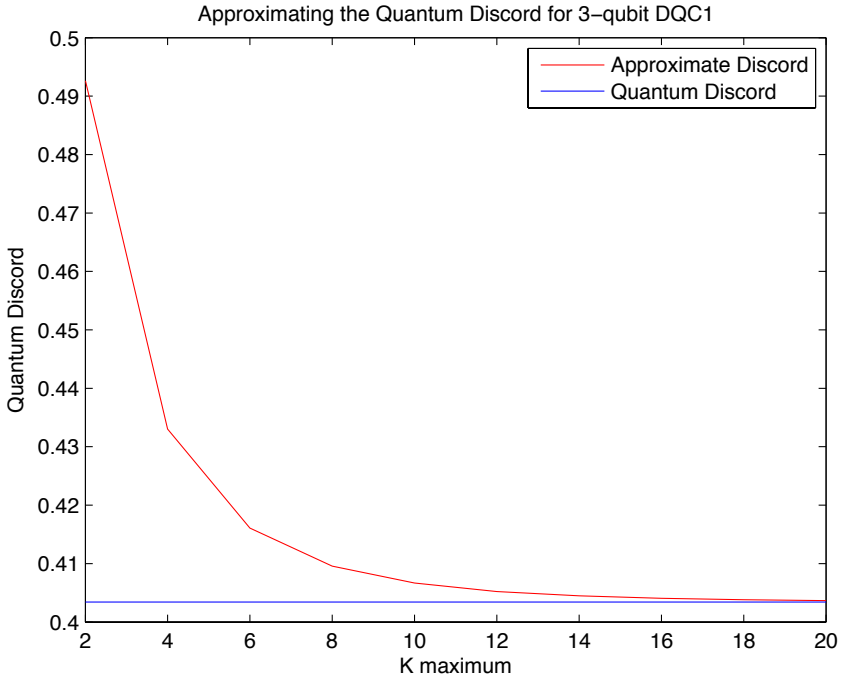

Figure C.1: Plot of the approximation of the quantum discord as a function of the number of series terms used to calculate it. This example is for a three-qubit DQC1-model where the two-qubit unitary on the bottom register was chosen at random from the Haar measure.

References

[AA11] D. Aharonov and I. Arad. The BQP-hardness of approximating the Jones polynomial. *New Journal of Physics*, 13:035019, 2011. 35

[AC+11] R. Auccaise, L.C. Celéri, , D.O. Soares-Pinto, E.R. deAzevedo, J. Maxiero, A.M. Souza, T.J. Bonagamba, R.S. Sarthour, I.S. Oliveira, and R.M. Serra. Environment-induced sudden transition in quantum discord dynamics. *Phys. Rev. Lett.*, 107:140403, 2011. 31

[AG11] G. Adesso and D. Girolami. Gaussian geometric discord. *Int. J. of Quant. Inf.*, 9:1993, 2011. 89

[AJL06] D. Aharonov, V.F.R. Jones, and Z. Landau. A polynomial quantum algorithm for approximating the Jones polynomial. STOC 06, 2006. 35

[Ale28] J.W. Alexander. Topological invariants of knots and links. *Trans. Amer. Math. Soc.*, 30(2):275–306, 1928. 34

[Ali10] M. Ali. Quantum discord for a two-parameter class of states in $2 \otimes d$ quantum systems. *J. Phys. A: Math. Theor.*, 43:495303, 2010. 80

[AMC+11] R. Auccaise, J. Maziero, L.C. Celeri, D.O. Soares-Pinto, E.R. deAzevedo, T.J. Bonagamba, R.S. Sarthour, I.S. Oliveira, and R.M. Serra. Experimentally witnessing the quantumness of correlations. *Phys. Rev. Lett.*, 107:070501, 2011. 67

[ARA10] M. Ali, A.R.P. Rau, and G. Alber. Quantum discord for two-qubit X states. *Phys. Rev. A.*, 81:042105, 2010. 81

[BBC+93] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895, 1993. 16

[BBC+95] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P.W. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457, 1995. 14

[BC10] B. Bylicka and D. Chruscinski. Witnessing quantum discord in $2 \times n$ systems. *Phys. Rev. A.*, 81:062102, 2010. 67

[BCCea07] J. Baugh, J. Chamilliard, C. M. Chandrashekar, and et. al. Quantum information processing using nuclear and elctron magnetic resonance: Review and prospects. *Physics in Canada*, Special Issue on Quantum Computing and Quantum Information, 2007. 9

[BCJ+99] S.L. Braunstein, C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.*, 83(5):1054, 1999. 18, 19

[BPM+97] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997. 1

[BPPC11] J. Batle, A. Plastino, A.R. Plastino, and M. Casas. Peculiarities of quantum discord's geometric measure. *J. Phys. A: Math. Theor.*, 44:505304, 2011. 89, 96

[CL03] D.P. Chi and S. Lee. Entanglement for a two-parameter class of states in $2 \otimes n$ quantum system. *J. Phys. A: Math. Gen.*, 36:11503–11511, 2003. 81

[CLL04] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004. 16

[CMS11] L.C. Celéri, J. Maziero, and R.M. Serra. Theoretical and experimental aspects of quantum discord and related measures. *International Journal of Quantum Informatoin*, 9:1837, 2011. 28

[CT06] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley-Interscience, 2006. 20

[CVZ+98] I.L. Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393:143–146, 1998. 1, 9

[CYC06] Z. Chen, J. Yepez, and D.G. Cory. Simulation of the Burgers equation by NMR quantum-information processing. *Phys. Rev. A.*, 74:042321, 2006. 1

[CZY+11] Q. Chen, C. Zhang, S. Yu, X.X. Yi, and C.H. Oh. On the quantum discord of two-qubit X-states. *Phys. Rev. A*, 84:042313, 2011. 81

[Dat08] A. Datta. *Studies on the Role of Entanglement in Mixed-state Quantum Computation*. PhD thesis, University of New Mexico, arXiv:0807:4490, 2008. 25, 64

[Dat10] A. Datta. A condition for the nullity of quantum discord. arXiv:1003.5256, 2010. 65

[DFC05] A. Datta, S.T. Flammia, and C.M. Caves. Entanglement and the power of one qubit. *Phys. Rev. A*, 72:042316, October 2005. 19, 30, 95

[DG09] A. Datta and S. Gharibian. Signatures of nonclassicality in mixed-state quantum computation. *Phys. Rev. A.*, 79:042325, 2009. 30

[Dia03] R. Diaconis. Patterns in eigenvalues: The 70th Josiah Willard Gibbs Lecture. *Bull. Amer. Math. Soc.*, 40:155–178, 2003. 101

[DiV95] D.P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A*, 51:1015, 1995. 14

[DSC08] A. Datta, A. Shaji, and C.M. Caves. Quantum discord and the power of one qubit. *Phys. Rev. Lett.*, 100:050502, 2008. 30, 62, 68, 82, 95, 101, 102

[DV07] A. Datta and G. Vidal. Role of entanglement and correlations in mixed-state quantum computation. *Physics Letters A*, 75:042310, 2007. 30

[DVB10] B. Dakic, V. Vedral, and C. Brukner. Necessary and sufficient condition for nonzero quantum discord. *Phys. Rev. Lett.*, 105:190502, 2010. 3, 28, 67, 76, 79, 82, 87, 95, 116, 120

[FAC+10] A. Ferraro, L. Aolita, D. Cavalcanti, F.M. Cucchietti, and A. Acín. Almost all quantum states have nonclassical correlations. *Phys. Rev. A*, 81:052318, 2010. 31, 62, 66, 79

[FKW02] M.H. Freedman, A. Kitaev, and Z. Wang. Simulation of topological field theories by quantum computers. *Commun. Math. Phys.*, 227:587 – 603, 2002. 35

[FLW02] M.H. Freedman, M. Larsen, and Z. Wang. A modular functor which is universal for quantum computation. *Commun. Math. Phys.*, 227:605 – 622, 2002. 35

[GA11a] D. Girolami and G. Adesso. Interplay between computable measures of entanglement and other quantum correlations. *Phys. Rev. A*, 84:052110, 2011. 89

[GA11b] D. Girolami and G. Adesso. Observable measure of quantum correlations. arXiv:1110.5083, 2011. 88, 89

[GA11c] D. Girolami and G. Adesso. Quantum discord for general two-qubit states: Analytical progress. *Phys. Rev. A.*, 83:052108, 2011. 81, 89

[GPA11] D. Girolami, M. Paternostro, and G. Adesso. Faithful nonclassicality indicators and extremal quantum correlations in two-qubit states. *J. Phys. A: Math. Theor.*, 44:352002, 2011. 28

[GPW05] B. Groisman, S. Popescu, and A. Winter. Quantum, classical, and total amount of correlations in a quantum state. *Physical Review A*, 72(3):32317, 2005. 28

[Gre07] L. Greenemeier. *Election fix? Switzerland Tests Quantum Cryptography.* Scientific American, October 19, 2007. 1

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1–8, 1996. 20, 63

[HHH+05] M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen, and B. Synak-Radtke. Local versus nonlocal information in quantum-information theory: Formalism and phenomena. *Physical Review A*, 71(6):62307, 2005. 28

[HHHH09] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865–942, 2009. 20

[HLP99] J. Hass, J. Lagarias, and N. Pippenger. The computational complexity of knot and link problems. *Journal of the AMC*, 46(2):185–211, 1999. 34

[HSR03] M. Horodecki, P.W. Shor, and M.B. Ruskai. Entanglement breaking channels. *Rev. Math. Phys.*, 15:629–641, 2003. 16

[HV01] L Henderson and V Vedral. Classical, quantum and total correlations. *J. Phys. A: Math. Gen.*, 34:6899–6905, 2001. 2, 22, 62, 80

[HW97] S. Hill and W.K. Wootters. Entanglement of a pair of quantum bits. *Phys. Rev. Lett.*, 78:5022, 1997. 19

[HWZ11] J.-H. Huang, L. Wang, and S.-Y. Zhu. A new criterion for zero quantum discord. *New Journal of Physics*, 13:063045, 2011. 65

[JL03] R. Jozsa and N. Linden. On the role of entanglement in quantum-computational speed-up. *Proc. R. Soc. Lond. A*, 459(2036):2011–2032, 2003. 16

[JM98] J.A. Jones and M. Mosca. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. *The Journal of Chemical Physics*, 109(5), 1998. 1, 9

[JMH98] J.A. Jones, M. Mosca, and R.H. Hansen. Implementation of a quantum search algorithm on a quantum computer. *Nature*, 393:344–346, 1998. 9

[Jon85] V.F.R. Jones. A polynomial invariant for knots via Von Neumann algrbras. *Bull. Amer. Math. Soc.*, 12(1):103–111, 1985. 34

[Jon01] J.A. Jones. NMR quantum computation. *Prog. NMR Spectrosc.*, 38:325–360, 2001. 9

[JVW90] F. Jaeger, D. L. Vertigan, and D. J. A. Welsh. On the computational complexity of the Jones and Tutte polynomials. *Mathematical Proceedings of the Cambridge Philosophical Society*, 108:35–53, 1990. 35

[JZYS11] J. Jin, F. Zhang, C. Yu, and H. Song. Direct scheme for measuring the geometric quantum discord. arXiv:1110.5693, 2011. 89

[Kau88] L.H. Kauffman. New invariants in the theory of knots. *American Mathematical Society*, 95(3):195–242, March 1988. 34

[Kau91] L.H. Kauffman. *Knots and Physics*. World Scientific, 1991. 3, 34

[KG11] G. Karpat and Z. Gedik. Correlation dynamics of qubit-qutrit systems in a classical dephasing environment. *Phys. Lett. A*, 375:4166–4171, 2011. 89

[KJ07] L.H. Kauffman and S.J. Lomonaco Jr. A 3-stranded quantum algorithm for the Jones polynomial. In *Proceeding SPIE, Vol. 6573*, 2007. 35

[KL98] E. Knill and R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81(25):5672, 1998. 2, 13, 19

[KL07] L.H. Kauffman and S.J. Lomonaco. q-Deformed spin networks, knot polynomials and anyonic topological quantum computation. arXiv:0606114, 2007. 44

[KLM07] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007. 34

[KRK+05] N. Khaneja, T. Reiss, C. Kehlet, T. Schulte-Herbruggen, and S. Glaser. Optimal control of coupled spin dynamics: Design of NMR pulse sequences by gradient ascent algorithms. *J. Magn. Reson.*, 172:296–305, 2005. 11, 125

[LBAW08] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White. Experimental quantum computing without entanglement. *Phys. Rev. Lett.*, 101:200501, 2008. 30, 68

[LBF98] N. Linden, H. Berjat, and R. Freeman. An implementation of the Deutsch-Jozsa algorithm on a three-qubit NMR quantum computer. *Chem. Phys. Lett.*, 296:61–67, 1998. 1

[Lev08] M.H. Levitt. *Spin Dynamics: Basics of Nuclear Magnetic Resonance*. John Wiley and Sons Ltd, 2008. 9

[LF10] S. Luo and S. Fu. Geometric measure of quantum discord. *Phys. Rev. A.*, 82:0343022, 2010. 88

[LM04] G.M. Leskowitz and L.J. Mueller. State interrogation in nuclear magnetic resonance quantum-information processing. *Physical Review A*, 69(5):52302, 2004. 71

[LMXW11] X.-M. Lu, J. Ma, Z. Xi, and X. Wang. Optimal measurements to access classical correlations of two-qubit states. *Phys. Rev. A.*, 83:012327, 2011. 81

[LPB10] E.-M. Laine, J. Pillo, and H.-P. Breuer. Witness for initial system-environment correlations in open-system dynamics. *EPL*, 92:60010, 2010. 67

[Luo08] S. Luo. Quantum discord for two-qubit systems. *Phys. Rev. A.*, 77:042303, 2008. 80

[LZ09] S. Luo and Q. Zhang. Observable correlations in two-qubit states. *J. Stat. Phys.*, 136(1):165–177, 2009. 28

[MCC11] Z.-H. Ma, Z.-H. Chen, and J.-L. Chen. Witness to detect quantum correlation of bipartite states in arbitrary dimension. arXiv:1104.0299, 2011. 67

[MFK+10] R. Marx, A. Fahmy, L. Kauffman, S. Lomonaco, A. Sp orl, N. Pomplun, R. Schulte-Herbr uggen, J.M. Myers, and S.J. Glaser. Nuclear-magnetic-resonance quantum calculations of the Jones polynomial. *Phys. Rev. A.*, 81:032319, 2010. 35

[MPS+10] K. Modi, T. Paterek, W. Son, V. Vedral, and M. Williamson. Unified view of quantum and classical correlations. *Phys. Rev. Lett.*, 104:080501, 2010. 28

[MS10] J. Maziero and R.M. Serra. Classicality witness for two-qubit states. arXiv:1012.3075, 2010. 67

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 4

[NKL98] M.A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation by nuclear magnetic resonance. *Nature*, 396(6706):52–55, 1998. 1

[NSO+05] C. Negrevergne, R. Somma, G. Ortiz, E. Knill, and R. Laflamme. Liquid-state NMR simulations of quantum many-body problems. *Phys. Rev. A.*, 71:032344, 2005. 1

[OHHH02] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki. Thermodynamical approach to quantifying quantum correlations. *Phys. Rev. Lett.*, 89:180402, 2002. 28

[OZ01] H. Ollivier and W.H. Zurek. Quantum discord: A measure of the quantumness of correlations. *Phys. Rev. Lett.*, 88(1):017901, 2001. 2, 22, 23, 28, 62

[PHH08] M. Piani, P. Horodecki, and R. Horodecki. No-local-broadcasting theorem for multipartite quantum correlations. *Phys. Rev. Lett.*, 100:090502, 2008. 28

[PML12] G. Passante, O. Moussa, and R. Laflamme. Measuring geometric quantum discord using one bit of quantum information. *Phys. Rev. A*, 85(3):032325, 2012. 80

[PMRL09] G. Passante, O. Moussa, CA Ryan, and R. Laflamme. Experimental approximation of the Jones polynomial with one quantum bit. *Physical Review Letters*, 103(25):250501, 2009. 35

[PMTL11] G. Passante, O. Moussa, D.A. Trottier, and R. Laflamme. Experimental detection of nonclassical correlations in mixed-state quantum computatation. *Phys. Rev. A*, 84:044302, 2011. 63

[RLL09] C.A. Ryan, M. Laforest, and R. Laflamme. Randomized benchmarking of single- and multi-qubit control in liquid-state NMR quantum information processing. *New Journal of Physics*, 11:013034, 2009. 1, 9, 33

[RNL+08] C.A. Ryan, C. Negrevergne, M. Laforest, E. Knill, and R. Laflamme. Liquid-state nuclear magnetic resonance as a testbed for developing quantum control methods. *Phys. Rev. A*, 78(1):012328, 2008. 11, 125

[RS10] R. Rahimi and A. SaiToh. Single-experiment-detectable nonclassical correlation witness. *Phys. Rev. A.*, 82:022314, 2010. 67

[Rya08] C.A. Ryan. *Characterization and Control in Large Hilbert Spaces*. PhD thesis, University of Waterloo, 2008. 11, 55, 125

[SBC+11] A. Smirne, D. Brivio, S. Cialdi, B. Vacchini, and M.G.A. Paris. Experimental investigation of initial system-environment correlations via trace distance evolution. *Phys. Rev. A.*, 84:032112, 2011. 67

[SJ08] P.W. Shor and S.P. Jordan. Estimating Jones polynomials is a complete problem for one clean qubit. *Quantum Information and Computation*, 8(8/9):681–714, 2008. 35, 44, 47, 49, 51, 52, 61

[SJSD11] M. Shi, F. Jiang, C. Sun, and J. Du. Geometric picture of quantum discord for two-qubit states. *New Journal of Physics*, 13:073016, 2011. 28

[SKF83] A.J. Shaka, J. Keeler, and R. Freedman. Evaluation of a new broadband decoupling sequence: Waltz-16. *Journal of Magnetic Resonance*, 53:313–340, 1983. 53, 125

[SPCA+10] D.O. Soares-Pinto, L.C. Celéri, R. Auccaise, F.F. Fanchini, E.R. deAzevedo, J. Maxiero, T.J. Bonagamba, and R.M. Serra. Nonclassical correlation in NMR quadrupolar system. *Phys. Rev. A.*, 81:062118, 2010. 31

[STH+99] S. Somaroo, C.H. Tseng, T.F. Havel, R. Laflamme, and D.G. Cory. Quantum simulations on a quantum computer. *Phys. Rev. Lett.*, 83:5381–5384, 1999. 1

[SZRL11] A.M. Souza, J. Zhang, C.A. Ryan, and R. Laflamme. Experimental magic state distillation for fault-tolerant quantum computing. *Nature Communications*, 2(169), 2011. 1

[Ter00] B.M. Terhal. Bell inequalities and the separability criterion. *Phys. Lett. A*, 271:319–326, 2000. 20, 63

[TSS+99] C. H. Tseng, S. Somaroo, Y. Sharf, E. Knill, R. Laflamme, T. F. Havel, and D. G. Cory. Quantum simulation of a three-body-interaction Hamiltonian on an NMR quantum computer. *Phys. Rev. A.*, 61:012302, 1999. 1

[VC04] L. M. K. Vandersypen and I. L. Chuang. NMR techniques for quantum control and computation. *Rev. Mod. Phys.*, 76:1037, 2004. 9

[Vid03] G. Vidal. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.*, 91:147902, 2003. 16

[VR11] S. Vinjanampathy and A.R.P. Rau. Calculation of quantum discord for qubit-qudit or n qubits. arXiv:1106.4488, 2011. 88

[VSB+01] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magentic resonance. *Nature*, 414:883–887, 2001. 1

[VW02] G. Vidal and R.F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, 2002. 19

[WG11] Y.-C. Wu and G.-C. Guo. Norm-based measurement of quantum correlation. *Phys. Rev. A.*, 83:062301, 2011. 28

[Woo98] W.K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245, 1998. 19

[WY08] P. Wocjan and J. Yard. The Jones polynomial: Quantum algorithms and applications in quantum complexity theory. *Quant. Inf. Comput*, 8:0147–0180, 2008. 35

[Xu11] J. Xu. Geometric measure of quantum discord over two-sided projective measurements. *Phys. Lett. A*, 376:320–324, 2011. 28

[YZCO11] S. Yu, C. Zhang, Q. Chen, and C.H. Oh. Witnessing the quantum discord of all the unknown states. arXiv:1102.4710, 2011. 67

[ZHSL98] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of spearable states. *Phys. Rev. A*, 58:883, 1998. 19