Collective Dynamics in NMR and Quantum Noise

by

Razieh Annabestani

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

Waterloo, Ontario, Canada, 2016

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.

R. Annabestani

Abstract

We introduced an open quantum system model to describe the statistical fluctuations of a spin ensemble in NMR. The model considers an ensemble measurement where the detection coil does not distinguish spins, and accounts for the state update rule. The analysis brings clarity and accuracy in describing the notion of spin noise and derives a correct statistical distribution and correlation function for the spin noise signal.

We propose a proof-of-principle experiment to encode one logical qubit in the noise protected subspace of three identical spins in a methyl group. We use a symmetry analysis to derive the dipole moment allowed transitions, which enable us to access the noiseless subsystem. We further analyze the symmetry of the hetronuclear dipolar relaxation, which is one of the responsible mechanisms for observing a noise protected state. Our analytical calculations predict features of of the NMR peaks that are in agreement with the experimental observations.

We propose a quantum key distribution protocol that simplifies the task of classical data processing in a trusted relay network. A new announcement strategy is proposed which leads to reassigning the task of error correction and privacy amplification from the intermediate user to the end-node users. We examine the security of the proposed protocol analytically, derive the key rate for two well-known examples of BB84 and 6-state protocols numerically, and consider a few imperfections arising in practical QKD.

Acknowledgements

First all, I would like to express my sincere appreciation to my supervisor Dr. David Cory who gave me the opportunity to complete my PhD study at Institute for Quantum Computing. I benefit from his advice, guidance, knowledge and experiences to accomplish my projects. His support assisted me to manage my family life while studying. I must also thank Dr. Norbert Lütkenhaus who supervised me for almost a year and half of my PhD program. I am grateful for his support and advice, for giving me the chance to attend QCrypt conference and for providing the opportunity to peruse my passion in physics.

Further thanks goes to my advisory committee members, Dr. Jonathan Baugh, Dr.Thomas Jennewein, Dr. Michele Mosca, and Dr. Ashwin Nayak for sharing their knowledge and making insightful comments during the committee meetings. A special thank to Dr. Joseph Emerson whose information was a great help to understand foundational concepts in quantum mechanics. I would like to thank Dr. Pierre-Nicholas Roy and Dr. Gregory S. Boutic for participating in my graduating committee.

The friendship with my colleagues at IQC made these years a pleasant memory for my future and the scientific discussions with them lightened my eyes to look at my research from various angles. I would like to thank Dr. Varun Narasimhachar, Maryam Mirkamali, Dr. Robabeh Rahimi Darabad, Dr. Agnes Ferenczi, Dr. Peter Groszkowski, Jean-Luc FX. Orgiazzi, Dr. Jean-Philippe Bourgoin, Dr. Juan Miguel Arrazola, Dr. Christopher Wood, Ian Hincks, Dr. George Nichols, Mohammad Niknam, Rahul Deshpande and Kamyar Ghofrani.

I am indebted to my parents and siblings who have always encouraged me to pursue my goals. They walked with me side by side during this long path from elementary school to PhD and felt the pain of of going up the barriers and the joy of success afterwards. I would like to thank Somayeh Nademi, Fatemeh Dorri and Sayeh Rajabi who are as sisters to me, for their endless kindness, motivation and support along the way.

Last but not least, I express a deep sense of gratitude to my husband Vahid Johari who has always held my back like a father, dedicated his life to me like a mother and encouraged and inspired me like a friend. I would not accomplish anything in my career without his endless love. Thank you for making my life meaningful.

Dedication

I dedicate this thesis to my dear siblings, Fatemeh and Reza, whose souls live in my heart and to my loves, Vahid and Helena, whose hearts live in my soul.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

"*The physical world is quantum mechanical, and therefore the proper problem is the simulation of quantum physics*", stated Richard Feynman in 1982 [1]. His observation inspired the field of quantum information processing (QIP) with the ultimate goal of building a quantum computer (QC). A QC is believed to increase the efficiency of solving certain computational problems in addition to simulating physics [2]. At present, there remains a long pathway to building a *universal quantum computer*, however, the advances in QIP have enriched physics and engineering through the development of new theoretical tools and even commercial applications such as spin based imaging and quantum key distribution [3, 4].

Over the past decades, there have been several proposals for physical implementations of a quantum processor including trapped ions, superconducting qubits, and spins [5–7]. All of these physical systems are extremely sensitive to environmental noise, which limits their utility as qubits. Theories of open quantum systems have been developed in QIP to effectively model the dynamics of a system which is coupled to an environment with several inaccessible and unknown degrees of freedom. This thesis uses the theory of open quantum systems to model the process of measuring an ensemble of spins that are identically coupled to a detection device [8]. This type of measurement arises in nuclear magnetic resonance (NMR). The NMR signal is normally treated as the average value of the total spin magnetic moment, because spins are weakly coupled to an NMR detection coil. We introduce a quantum model that keeps track of each instance of the measured total magnetic moment of the ensemble, accounts for the evolution of this open quantum system, and applies the state update rule. This model leads to a clear and accurate description of the quantum fluctuations of the spin ensemble, known as *spin noise signal*.

One of the crucial challenges in QIP is protecting the quantum processor from undesired couplings to its environment, which manifest themselves as a noise process on the physical system

of interest. This motivates another branch of QIP, known as quantum error correction (QEC) whose aims are to both retrieve quantum information that is corrupted by noise, and to protect it against noise. NMR, owing to its long history, has been among the first physical candidates to experimentally demonstrate the quantum information and error correction algorithms [9–12]. One of the concepts developed in QEC is the notion of *noiseless subsystems*, where information is encoded in a particular way so as to have noise immunity. This thesis investigates an NMR implementation of a noiseless quantum state that is created by using the collective properties of a group of indistinguishable spins. In particular, a symmetry analysis of methyl groups suggests that a group of three identical protons can serve as one logical qubit that is immune to collective noise. Our analysis not only offers a practical way for implementing a noise protected quantum processor, but also provides an enriched understanding of the relaxation mechanisms that lead to an NMR observation of a noiseless state.

The emergence of QIP with the promise of building a quantum computer threatens the security of existing classical cryptography protocols. For example, if a fault tolerant quantum computer is ever constructed, Shor's algorithm, which can factor large numbers into their prime components exponentially more efficient than known classical counterparts, is a threat to the RSA protocol [2]. Quantum Key Distribution (QKD) is a branch of quantum cryptography that aims to generate secret keys and share them between two remote parties. The security of the QKD protocols relies fundamentally on the laws of quantum mechanics, which is in contrast to the classical key distribution protocols whose security relies on hardness of solving a mathematical problem.

It is desired to establish a secret key between two legitimate users who are located on any part of the globe, but practically, the range of a direct link QKD is presently limited to a few hundred kilometers. One solution is a quantum network that consists of multiple users to extend the range of QKD to an arbitrary distance [13, 14]. However, this introduces other significant experimental challenges such as having access to a perfect quantum memory, or the need for considerable communication and computational resources at intermediate nodes. This thesis proposes a simplified trusted relay (STR) protocol that integrates a particular announcement strategy to reassign the task of quantum error correction and privacy amplification from the intermediate nodes to the legitimate users. An STR quantum key distribution is a variation of a trusted relay network with the advantage of significant reduction in the required classical computation and communication resources at intermediate nodes [15].

The outline of this thesis is as follows: Chapter 2 reviews the main postulates of quantum mechanics, clarifying each notion by providing an explanation of it in the NMR context. In Chapter 3, we provide an open quantum system model to describe the origin of the spin noise signal. In Chapter 4, we explore the possibility of experimental demonstration of a noise protected state in a methyl group. In Chapter 5, we provide a theoretical security proof of a simplified trusted

relay QKD protocol.

Acknowledgement of Contributions

- Chapter 3 contains results published in [8] which was a work in collaboration with David G. Cory and Joseph Emerson.
- Chapter 4 contains unpublished results of the author.
- Chapter 5 contains main contribution of the author to the results publised in [15]. This work was done in collaboration with William Stacey, Xiongfeng Ma and Norbert Lütkenhaus.

Chapter 2

Postulates of Quantum Mechanics

Quantum mechanics is a mathematical framework that provides a theoretical description of physical phenomenon. During the past century, several fundamental experiments, such as Bell inequality violations [16–18] have been conducted to show the consistency between this mathematical framework and the experimental observations. There are three main postulates of quantum mechanics that mathematically describe the physical processes of quantum systems, *state preparation, evolution* and *measurement*. Ideally, it is assumed that the quantum system of interest is fully isolated from the rest of the world, and so is a *closed* system. In reality, the system of interest is interacting with its *environment*, and so is an *open* quantum system. This chapter reviews the postulates of quantum mechanics in both closed systems and open quantum systems, clarifying the concept of each postulate by providing its correspondence in the NMR context.

2.1 Mathematical Preliminaries

Definition 2.1. A finite d-dimensional Hilbert space $\mathscr{H}_d$ is defined as a vector space of complex numbers $\mathbb{C}$ with an inner product, and is complete in norm.

Completeness in norm of a finite vector space $\{v_n | v_n \in \mathscr{H}\}$, means that $v = \lim_{n\to\infty} v_n \in \mathscr{H}$.

In Dirac notation, a d-dimensional vector $v \in \mathscr{H}_d$ is represented by a *ket* $|v\rangle$, and its complex conjugate (transpose) is represented by a *bra* $\langle v| = |v\rangle^\dagger$ which is an element of the *dual* Hilbert space. Considering this notation, the inner product of a vector space has the following properties,

1. $\langle v|v\rangle \geq 0$.

2. $\langle w|v\rangle \in \mathbb{C}$.

3. $\langle w|v\rangle = \langle v|w\rangle^*$.

4. $\langle w|c_1\ v_1 + c_2\ v_2\rangle = c_1\ \langle w|v_1\rangle + c_2\ \langle w|v_2\rangle$.

Definition 2.2. An operator $\hat{A}$ is self-adjoint or Hermitian iff $\hat{A}^\dagger = \hat{A}$. The symbol † denotes conjugate transpose.

Definition 2.3. An operator $\hat{U}$ is unitary iff $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbb{1}$.

Definition 2.4. An orthonormal basis, ON$= \{v_1, v_2, ..., v_n\}$, for a vector space V with inner product $\langle\ ,\ \rangle$ is a set of linearly independent vectors that are orthogonal with length one, i.e., $\langle v_i, v_j\rangle = \delta_{ij}$. This subset, ON$\subset V$ constructs a basis, because an arbitrary vector $w \in V$ can be expanded in terms of these orthonormal vectors.

Definition 2.5. Given an orthonormal basis $\{|i\rangle\}$, the trace of $\hat{A}$ is given by

$$Tr[\hat{A}] = \sum_i \langle\ i\ |\hat{A}|\ i\ \rangle. \tag{2.1}$$

Definition 2.6. We denote the set of all linear operators acting on $\mathscr{H}$ by $\mathbf{L}(\mathscr{H})$. A density matrix or density operator $\rho \in \mathbf{L}(\mathscr{H})$, is a positive semidefinite operator and has unit trace. The set of all density matrices acting on $\mathscr{H}$ is denoted by $\Gamma(\mathscr{H}) \subset \mathbf{L}(\mathscr{H})$,

$$\Gamma(\mathscr{H}) := \{\rho \in \mathbf{L}(\mathscr{H})|\ \rho \geq 0\ \&\ Tr[\rho] = 1\}. \tag{2.2}$$

Definition 2.7. Consider the Hilbert space of a composite system, $\mathscr{H}_{SE} = \mathscr{H}_S \otimes \mathscr{H}_E$, where the symbol $\otimes$ denotes the tensor product of the two spaces. The partial trace of $\hat{A} \in \mathbf{L}(\mathscr{H}_{SE})$ is defined by

$$\begin{aligned} Tr_E[\hat{A}] &= \sum_i (\mathbb{1} \otimes \langle i_E|)\ \hat{A}\ (\mathbb{1} \otimes\ |i_E\rangle), \\ Tr_S[\hat{A}] &= \sum_i (\langle i_S| \otimes \mathbb{1})\ \hat{A}\ (|i_S\rangle \otimes\ \mathbb{1}), \end{aligned} \tag{2.3}$$

where $\{|i_S\rangle\}$ and $\{|i_E\rangle\}$ are two sets of orthonormal bases that are defined on $\mathscr{H}_S$ and $\mathscr{H}_E$ respectively.

Definition 2.8. A linear map $\mathscr{E} : \mathbf{L}(\mathscr{H}) \to \mathbf{L}(\mathscr{H})$ is trace preserving iff $Tr[\rho] = Tr[\mathscr{E}[\rho]]$ for all $\rho \in \mathbf{L}(\mathscr{H})$.

Definition 2.9. A linear map $\mathscr{E} : \mathbf{L}(\mathscr{H}_S) \to \mathbf{L}(\mathscr{H}_S)$ is positive iff $\forall \rho \geq 0$, $\mathscr{E}[\rho] \geq 0$, and it is *completely positive* (CP) iff $\mathbb{1} \otimes \mathscr{E} : \mathbf{L}(\mathscr{H}_{SE}) \to \mathbf{L}(\mathscr{H}_{SE})$ is positive.

Definition 2.10. Given a matrix $A = \sum_{ij} a_{ij} \, |i\rangle\langle j|$ where $\{|i\rangle\}$ is an orthonormal basis, we define the column-vector and the row-vector representation of A by

$$\begin{aligned} \|A \, \rangle\!\rangle_c &= \sum_{ij} a_{ji} \, |i\rangle \otimes |j\rangle, \\ \|A \, \rangle\!\rangle_r &= \sum_{ij} a_{ij} \, |j\rangle \otimes |i\rangle. \end{aligned} \tag{2.4}$$

In the *Liouville* representation, a $d \times d$ matrix A is represented by a $1 \times d^2$ vector $\|A \, \rangle\!\rangle$. An important consequence of the vectorization definition is the Roth's Lemma, which states that $\|A \; \rho \; C \, \rangle\!\rangle_c = C^T \otimes A \, \|\rho \, \rangle\!\rangle_c$, where superscript T is the transposition transformation [19]. Consequently, considering the column vectorization convention, the Liouville representation of any map $\mathscr{E}[.] = A \; . \; C$ with size $d \times d$ is a *linear superoperator* $\hat{\hat{\mathscr{E}}} = C^T \otimes A$ with size $d^2 \times d^2$.

2.2 Postulate I: Quantum State

In the first postulate of quantum mechanics, the state of a physical system is described by an assigned vector or an assigned matrix. For every d-level quantum system that has a *pure* state, a d-dimensional normalized vector $|\psi\rangle \in \mathscr{H}_d$ is assigned. Alternatively, a pure state is represented by a density matrix $\rho = |\psi\rangle\langle\psi| \in \Gamma(\mathscr{H})$. One may consider a mixture of pure states $|\psi_x\rangle$ that are each prepared with probability $p(x)$. In that case the quantum system can no longer be described by a pure state. By definition, any state that is not *pure* is a *mixed* state. In general, to every d-level quantum system a $d \times d$ density matrix $\rho \in \Gamma(\mathscr{H})$ is assigned .

Theorem 2.11. *Any mixed state can be written as a convex combination of pure states, i.e.,* $\rho = \sum_x p(x) \, |\psi_x\rangle\langle\psi_x|$ *[20].*

Note that for any arbitrary $\rho \in \Gamma(\mathscr{H})$, we have $\frac{1}{d} \leq Tr[\rho^2] \leq 1$. The lower bound belongs to a maximally mixed state $\rho_0 = \frac{\mathbb{1}}{d}$, and the upper bound belongs to a totally pure state $\rho_1 = |\psi\rangle\langle\psi|$, because, $\rho_1^2 = \rho_1$ and $Tr[\rho_1^2] = 1$. Therefore, $Tr[\rho^2]$ provides a practical way of testing how much *purity* a quantum state has.

2.2.1 Composite system

Consider two physical systems A and B. The density matrix describing the state of this composite system is denoted by $\rho_{AB} \in \Gamma(\mathscr{H}_{AB})$ where the joint Hilbert space $\mathscr{H}_{AB}$ is defined as the tensor-product of each individual system's Hilbert spaces, i.e. $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$. Studying the dynamics of a part of a composite system, requires that the *reduced* density matrix be defined.

Definition 2.12. Given the density matrix of a composite system ρ_{AB}, the state of the subsystem A is defined by $\rho_A = Tr_B[\rho_{AB}]$ where Tr_B is the partial trace over the subsystem B. Similarly, $\rho_B = Tr_A[\rho_{AB}]$.

A composite system may appear in various states:

1. **Product States:** Two systems, A and B, are independent and have no quantum and classical correlation iff $\rho_{AB} = \rho_A \otimes \rho_B$.

2. **Separable States:** A composite system is *separable* if the corresponding density matrix can be written as a convex combination of product states, i.e.

$$\rho_{AB} = \sum_x p(x)\ \rho_A^x \otimes \rho_B^x. \tag{2.5}$$

   A product state is a special case of separable states.

3. **Entangled States:** If a state is not separable, it is *entangled*.

Definition 2.13. For two sets of orthonormal bases $\{|i_A\rangle\} \in \mathscr{H}_A$ and $\{|i_B\rangle\} \in \mathscr{H}_B$, a maximally entangled state or a *Bell state* is defined by

$$|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_i |i_A\rangle \otimes |i_B\rangle. \tag{2.6}$$

Here, d is the dimension of each Hilbert space.

Entanglement is a sufficient condition for establishing quantum correlation between two subsystems, but it is not a necessary condition. Some separable states have non zero quantum correlations [21]. Non classical correlations versus entanglement is an active field of research but is beyond the scope of this thesis.

2.2.2 Quantum States in NMR

NMR studies magnetic properties of various spin species. In particular, a spin half particle is a two-level system that is a candidate for quantum information processing (qubit). In the presence of a static magnetic field, a spin half is either aligned or anti-aligned with the field, and the corresponding pure states are,

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.7}$$

An arbitrary pure state is represented by $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$, with $\sqrt{|\alpha|^2 + |\beta|^2} = 1$, which is a coherent superposition of the spin basis. An arbitrary mixed state is represented by

$$\rho = \frac{1}{2}(\mathbb{1} + a_x\ \sigma_x + a_y\ \sigma_y + a_z\ \sigma_z), \tag{2.8}$$

where $\vec{a} = (a_x, a_y, a_z)$ is a real vector, and σ represents Pauli operators that are given by

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.9}$$

Pauli operators have some interesting properties: they are traceless $Tr[\sigma] = 0$; their square is an identity $\sigma^2 = \mathbb{1}$; they do not commute with each other $[\sigma_\alpha, \sigma_\beta] = 2i\ \varepsilon_{\alpha\beta\gamma}\ \sigma_\gamma$, and they anti-commute $\{\sigma_\alpha, \sigma_\beta\} = 0$ for all $\alpha, \beta, \gamma \in \{x, y, z\}$. Here, $[A, B] = AB - BA$ is the commutation of two operators, $\{A, B\} = AB + BA$ is the anti-commutation, and $\varepsilon_{\alpha\beta\gamma}$ is the Levi-Civita symbol. The set of $\{\frac{\mathbb{1}}{2}, S_x, S_y, S_z\}$ with $S_i = \frac{\sigma_i}{2}$ forms a basis for matrices, and any 2×2 matrix can be expanded in terms of them. These properties of Pauli operators result in $a_i = \langle\sigma_i\rangle = Tr[\sigma_i\ \rho]$ for $i \in \{x, y, z\}$. In addition, we obtain $0 \leq |\vec{a}| \leq 1$, where the lower bound corresponds to a maximally mixed state and the upper bound corresponds to pure states. Therefore, one can visualize the space of all density matrices of a two-level system or $\Gamma(\mathscr{H}_2)$ by a unit sphere known as the *Bloch sphere* in which every single point $\vec{a}$, corresponds to a density matrix $\rho \in \Gamma(\mathscr{H}_2)$. The Bloch sphere is depicted in Figure 2.1.

At equilibrium, the statistical information about a single spin half particle in the presence of static field $\vec{B}_0 = B_0\ \hat{z}$ and at temperature T, is given by a Boltzmann distribution. The interaction of a single spin with the static field is given by the *Zeeman* Hamiltonian, $H_0 = \vec{\mu}.\vec{B}_0$, where $\vec{\mu} = \hbar\gamma\ \vec{S}$ is the magnetic moment operator of a spin half particle. The associated density matrix at equilibrium is

$$\begin{aligned} \rho_0 &= \frac{e^{-\beta H_0}}{\mathscr{Z}}, \\ &= \frac{1}{2}(\mathbb{1} + \varepsilon_0 \sigma_z), \end{aligned} \tag{2.10}$$

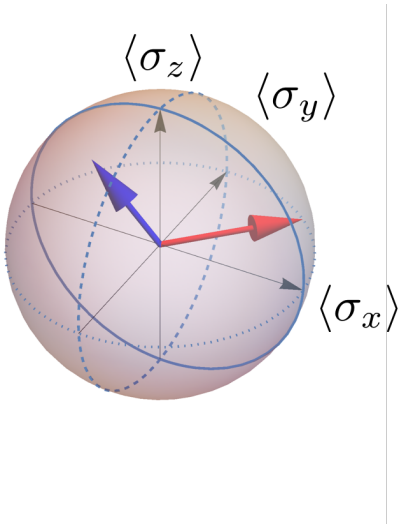

Figure 2.1: Bloch Sphere: A space of all density matrices of a two level system. The red arrow represents a pure state on the surface which is in the x-y plane and the blue arrow represents a mixed state which is inside the sphere.

where $\mathscr{Z}$ is a normalization factor, $\beta = 1/k_bT$ with k_b being the Boltzmann constant, and $\varepsilon_0 = \tanh[\frac{\hbar\gamma B_0}{2k_bT}]$ is the Boltzmann polarization. Normally, this polarization is very small. For example, at $B_0 = 10$ T and $T = 4$ K, a proton is polarized by 4×10^{-4}. The corresponding point on the Bloch sphere is a very little vector near the center (highly mixed state) that heads up towards the north of the sphere. According to Theorem 2.11, this mixed state can be interpreted as a sum of pure states that are all distributed across the Bloch sphere in such a way that on average they all are ε-oriented towards the north.

For an ensemble of N spin half particles, the total spin angular momentum is $\hbar\,\vec{\mathbf{S}} = \hbar\,(\vec{S}^{(1)} + \vec{S}^{(2)} + \cdots + \vec{S}^{(N)})$. Thus, the total Zeeman Hamiltonian is

$$H_{\text{Zeem}} = \hbar\gamma B_0\,\mathbf{S}_z. \tag{2.11}$$

Here, $\hbar\,\mathbf{S}_z = \hbar\sum_{i=1}^{N} S_z^{(i)}$ is the z component of the collective spin angular momentum, and $S_z^{(i)} = \frac{1}{2}\,(\mathbb{1}^{\otimes i-1} \otimes \sigma_z \otimes \mathbb{1}^{\otimes N-i})$. We use the bold notation to distinguish the collective spin operators

from the individual spin operators. Given H_{Zeem} , the equilibrium state of this spin ensemble is

$$\begin{aligned} \rho_{\text{ensm}} &= \frac{e^{-\beta H_{\text{Zeem}}}}{\mathscr{Z}}, \\ &= \frac{1}{\mathscr{Z}} \prod_i e^{-\beta\ \hbar\gamma B_0\ S_z^{(i)}}, \\ &= \rho_0^{\otimes N}. \end{aligned} \tag{2.12}$$

As we expected, the density matrix of an ensemble of non-interacting identical spins is a tensor product of each spin's density matrix. The polarization of this ensemble is thus, $\varepsilon = N\ \varepsilon_0 = N\ \tanh[\frac{\hbar\gamma B_0}{2k_bT}]$.

2.3 Postulate II: Evolution of Closed Quantum Systems

In the second postulate of quantum mechanics, the dynamic of a quantum state is described by a quantum evolution operator or a *propagator*. The dynamics of a *closed and pure* system is governed by the Schrödinger equation,

$$\frac{d|\psi(t)\rangle}{dt} = -i\,H\,|\psi(t)\rangle, \tag{2.13}$$

where H is the Hamiltonian of the system and we take $\hbar = 1$ and write the energies in frequencies. If H is time independent, the solution of the above differential equation is given by,

$$|\psi(t)\rangle = U(t)\,|\psi(0)\rangle \quad \text{, where} \quad U(t) = e^{-iH\ t}. \tag{2.14}$$

where the quantum evolution operator $U(t)$ is a unitary operator. The dynamics of *any closed* system including pure and mixed states is governed by the *von-Neumann* equation,

$$\frac{d\rho(t)}{dt} = -i\,[\,H,\,\rho(t)\,], \tag{2.15}$$

and its solution is given by $\rho(t) = U(t)\rho(0)U^\dagger(t)$ when the Hamiltonian is time-independent.

If H is time-dependent, the quantum evolution operator is $U(t) = \mathscr{T}\ e^{-i\int_0^t dt'\ H(t')}$ in which $\mathscr{T}$ is the time ordering operator. The Dyson series [22] expansion of $U(t)$ is

$$U(t) = \mathbb{1} - i\int_0^t dt_1\ H(t_1) + \frac{(-i)^2}{2!}\int_0^t dt_1 \int_0^{t_1} dt_2\ H(t_1)H(t_2) + \ldots \tag{2.16}$$

Note that a time ordering operator is required to make sure $t_1 \geq t_2 \geq t_3 \geq ...$, because, the Hamiltonian does not necessarily commute with itself at different times, i.e. $[\, H(t_1),\, H(t_2)\,] \neq 0$.

Average Hamiltonian Theory (AHT) and/or Magnus expansion looks for an average solution that at fixed time T, we get [22–24],

$$U(T) = \mathscr{T}\, e^{-i\int_0^T dt'\, H(t')} = e^{-i\mathbf{H}_{avg}T}, \tag{2.17}$$

where $\mathbf{H}_{avg} = \sum_{i=0} \mathbf{H}^{(i)}$ is an effective or an average Hamiltonian and $\mathbf{H}^{(i)}$ is the i^{th} order approximation. Just for the completeness of discussion, we provide the first few terms explicitly and refer to [25] for more details,

$$\begin{aligned} \mathbf{H}^{(0)} &= \frac{1}{T}\int_0^T dt_1\, H(t_1), \\ \mathbf{H}^{(1)} &= -\frac{1}{T}\frac{i}{2!}\int_0^T dt_1 \int_0^{t_1} dt_2\, [\, H(t_1),\, H(t_2)\,]. \end{aligned} \tag{2.18}$$

One can check that each order of the average Hamiltonian is a Hermitian operator. In general, there is no guarantee that the effective Hamiltonian converges [25]. Nevertheless, often the first few orders provide a good approximation of the physical system's dynamics.

2.3.1 Unitary Evolution in NMR

Consider a single spin in the presence of a static magnetic field along the z axis (the Zeeman term) and a time dependent RF field along the x axis that can be on or off (the control term). The Hamiltonian is

$$H = \frac{1}{2}\,(\omega_0\, \sigma_z + \omega_1\, \cos\omega_c t\, \sigma_x). \tag{2.19}$$

Here, $\omega_0 = \gamma B_0$ is the *Larmor* frequency, $\omega_1 = \gamma B_1$ is the *Rabi* frequency and ω_c is the *carrier* frequency. If we go to the interaction frame of $V_{\text{int}} = e^{i\frac{\omega_c}{2}t\ \sigma_z}$, the Hamiltonian in that frame becomes

$$\begin{aligned} \tilde{H} &= V_{\text{int}}\, H\, V_{\text{int}}^{\dagger} - \frac{1}{2}\omega_c\sigma_z, \\ &= \frac{1}{2}(\Delta\omega\sigma_z + \omega_1(\sigma_x + \cos 2\omega_c t\sigma_x - \sin 2\omega_c t\sigma_y)), \\ &\approx \frac{1}{2}(\Delta\omega\ \sigma_z + \omega_1\sigma_x), \end{aligned} \tag{2.20}$$

where $\Delta\omega = \omega_0 - \omega_c$ is the off-resonance frequency. In the last line we assumed $\omega_c \gg \Delta\omega$ and ω_1, and then, we ignored the fast oscillating terms. This is known as Rotating Wave Approximation (RWA).

Given the above RWA, one can implement a θ rotation pulse on the spin half system, by turning on a time oscillating RF field for a duration of τ so that $\omega_1\tau = \theta$ and setting the carrier frequency on resonance with the Larmor frequency, $\Delta\omega = 0$. For that choice of parameters, the quantum evolution operator is

$$\tilde{U}_\theta^{|x}(\tau) = e^{-i\tilde{H}\tau} = e^{-i\frac{\theta}{2}\sigma_x} = \cos\frac{\theta}{2}\,\mathbb{1} - i\,\sin\frac{\theta}{2}\,\sigma_x. \tag{2.21}$$

For $\theta = \frac{\pi}{2}$, the above pulse evolves an initial state $|\uparrow\rangle$ to $|-\rangle_y = \frac{1}{\sqrt{2}}(|\uparrow\rangle - i|\downarrow\rangle)$ state which correspond to a $\frac{\pi}{2}$ rotation around the x-axis on the Bloch sphere.

Typically, the detection part of an NMR experiment consists of a $\frac{\pi}{2}$ rotation pulse around an axis in the transverse plane (say $-y$) followed by a free evolution, taking an ε-polarized equilibrium state to

$$\begin{aligned} \rho_0 = \frac{1}{2}(\mathbb{1} + \varepsilon_0\,\sigma_z) \quad &\xrightarrow{\tilde{U}_{\pi/2}^{|-y}} \quad \frac{1}{2}(\mathbb{1} + \varepsilon_0\,\sigma_x), \\ &\xrightarrow{U_0} \quad \rho(t) = \frac{1}{2}(\mathbb{1} + \varepsilon_0\,(\cos\omega_0 t\;\sigma_x + \sin\omega_0 t\;\sigma_y)), \end{aligned} \tag{2.22}$$

where $U_0 = \exp[-i\frac{\omega_0}{2}t\;\sigma_z]$ is the free evolution due to the static field interaction. Ideally, in the absence of any relaxation or decoherence process, the spin system precesses around the z axis at rate ω_0 with no damping. This time dependent magnetization induces a time dependent voltage in the RF coil that is the NMR signal. This detection will be explained in more details in Section 2.5.3.

2.4 Postulate II: Evolution of Open Quantum Systems

Often, the physical system of interest with internal Hamiltonian H_S, is not fully isolated from the rest of the world or its *environment* with internal Hamiltonian H_E. Intuitively, when we just focus on the dynamic of the subsystem S and *ignore* the environment E, the expectation is that the term $-i[H_S, \rho_S]$ in the von-Neumann equation is not sufficient to describe the time evolution of this open system and there must be some footprints of environment's effect on the system. Mathematically, the composite system SE is a closed system that evolves by

$$\frac{d\rho_{SE}}{dt} = -i[\,H_{SE},\,\rho_{SE}\,], \tag{2.23}$$

where the total Hamiltonian $H_{SE} = H_S + H_E + H_{\text{int}}$ consists of internal Hamiltonians and an interaction term H_{int} due to the coupling between S and E. If we partial trace over the environment space in Equation (2.23) and under certain assumptions where basically the enviorment is assumed to be memoryless, the von-Neumann equation will be modified to a *quantum master* equation which governs the dynamics of an *open* quantum system. Specifically, under *Born-Markov approximation* [26], the quantum master equation reduces to

$$\frac{d\rho_S}{dt} = -i[\, H_S,\ \rho_S\,] + \hat{\mathscr{D}}[\rho_S]. \tag{2.24}$$

Here the extra term $\hat{\mathscr{D}}[.]$ is an effective map acting on the system alone which appears as a result of coupling with the environment.

There is two main assumptions in Markovian approximation: First, the system and the environment are not initially correlated, i.e., $\rho_{SE} = \rho_S \otimes \rho_E$, and second, the environment is memoryless, i.e., its action at time t_1 does not influence the dynamics at a later time $t_2 > t_1$. Hence, any information that leaks into a memoryless environment will be lost, and so, the map $\hat{\mathscr{D}}[.]$ is also known as a *dissipator*. A well known form of a Markovian master equation is the *Lindblad equation* in which the dissipator is [26]

$$\begin{aligned} \hat{\mathscr{D}}[\rho] &= \sum_i \gamma_i\, \hat{D}[L_i][\rho], \\ \text{where} & \\ \hat{D}[L_i][\rho] &= (L_i\, \rho L_i^\dagger - \frac{1}{2}\{L_i^\dagger L_i, \rho\}). \end{aligned} \tag{2.25}$$

L_i is called the *Lindbad operator* which generates a dissipative evolution $\hat{D}[L_i][\rho]$ at rate γ_i.

In general, the solution of a Markovian master equation is given by a linear map $\mathscr{E} : \mathbf{L}(\mathscr{H}) \to \mathbf{L}(\mathscr{H})$. This linear map represents a physical quantum evolution process that takes a density matrix to a density matrix, and hence, it must be a completely positive and trace preserving (CPTP) map and a unitary operator is a special case of a CPTP map. Various mathematical representations of a CPTP map is discussed in Section 2.6.

2.4.1 Master Equation in NMR

Redfield's theory derives a Markovian master equation in the weak coupling limit. The total Hamiltonian consists of a time independent term H_0 which is due to the internal interactions and is the dominant term, and a randomly varying term $H_1(t)$ which is due to the external interactions with the environment and in the weak coupling limit, $H_1(t)$ is treated as a perturbing term.

In a full quantum mechanical approach, both the system and the environment are treated quantum mechanically and the interaction Hamiltonian can be written as $H_1(t) = \sum_\alpha \hat{A}_\alpha \otimes \hat{g}_\alpha(t)$, where $\hat{A}_\alpha$ are operators acting on the system and $\hat{g}_\alpha(t)$ are time dependent operators acting on the environment. Using the Nakajima-Zwanzig equation and considering the Born-Markov approximation, the Redfield master equation [26] becomes

$$\frac{\partial \tilde{\rho}_S(t)}{\partial t} \approx -\int_0^\infty Tr_E[\,[\tilde{H}_1(t),[\tilde{H}_1(t-\tau),\tilde{\rho}_S(t)]\otimes\rho_E]\,]\,d\tau. \tag{2.26}$$

in which ρ_E is a fixed state and the tilde notation refers to the the rotating frame of $V = e^{iH_0 t}$, i.e., $\tilde{\rho} = V\rho V^\dagger$ and $\tilde{H}_1 = VH_1V^\dagger$. Normally, the environment has several inaccessible degrees of freedom which makes it difficult to use the quantum Redfield master equation for studying the system's dynamics.

In a semi-classical approach, the environment is treated as randomly varying classical functions and a second order perturbation theory is applied to derive the semi-classical Redfield master equation, [27], [28] and [29],

$$\frac{\partial \overline{\tilde{\rho}_S(t)}}{\partial t} \approx -\int_0^\infty \overline{[\tilde{H}_1(t),[\tilde{H}_1(t-\tau),\tilde{\rho}_S(t)]]}\,d\tau. \tag{2.27}$$

The overbar notation refers to the statistical averaging over the time dependent random variables. An example in the NMR context is when H_0 represents the Zeeman interaction at high field and $H_1(t)$ represents a coupling term (such as the dipolar interaction) that is decomposed as

$$H_1(t) = \sum_\alpha g_\alpha(t)\,\hat{A}_\alpha. \tag{2.28}$$

Here, $g^\alpha(t)$ is a randomly varying complex function and $\hat{A}_\alpha$ is a non-Hermitian operator with the following properties:

$$\begin{array}{ll} g_{-\alpha} = g_\alpha^* & [\,H_0,\,\hat{A}_\alpha] = \omega_\alpha\,\hat{A}_\alpha, \\ \hat{A}_{-\alpha} = \hat{A}_\alpha^\dagger & [\,H_0,\,\hat{A}_\alpha^\dagger] = -\omega_\alpha\,\hat{A}_\alpha^\dagger. \end{array} \tag{2.29}$$

Given the above relations, the interaction Hamiltonian in the rotating frame is

$$\begin{aligned} \tilde{H}_1(t) &= \sum_\alpha g_\alpha(t)\,e^{i\omega_\alpha t}\,\hat{A}_\alpha, \\ &= \sum_\alpha g_\alpha^*(t)\,e^{-i\omega_\alpha t}\,\hat{A}_\alpha^\dagger. \end{aligned} \tag{2.30}$$

Expanding the semi-classical Refield equation and replacing $\tilde{H}_1(t)$ result in

$$\begin{aligned}\frac{\partial\overline{\tilde{\rho}(t)}}{\partial t} &= \int_0^\infty \tilde{H}_1(t)\ \tilde{\rho}\ \tilde{H}_1(t-\tau) - \tilde{\rho}\tilde{H}_1(t-\tau)\ \tilde{H}_1(t) + h.c., \\ &= \sum_{\alpha,\beta}\Big(\int_0^\infty e^{i\omega_\alpha t}e^{-i\omega_\beta(t-\tau)}\overline{g_\alpha(t)g_\beta^*(t-\tau)}\ d\tau\Big)\ (\hat{A}_\alpha\ \tilde{\rho}\ \hat{A}_\beta^\dagger - \tilde{\rho}\ \hat{A}_\beta^\dagger\ \hat{A}_\alpha + h.c.)\end{aligned} \tag{2.31}$$

Now, we introduce the *correlation function* $R(\tau)$ and its Fourier transform $J(\omega)$,

$$\begin{aligned}R_{\alpha\beta}(\tau) &= \overline{g_\alpha(t)g_\beta^*(t+\tau)}, \\ J_{\alpha\beta}(\omega) &= \int_{-\infty}^\infty R_{\alpha\beta}(\tau)\ e^{-i\omega t}d\tau.\end{aligned} \tag{2.32}$$

$J(\omega)$ is the real part of the *spectral density of noise*. If we replace these definitions in Section 2.4.1 and do a secular approximation where only those terms are considered that $|\omega_\alpha - \omega_\beta|$ is negligible compare to $|H_0|$, we obtain

$$\begin{aligned}\frac{\partial\overline{\tilde{\rho}(t)}}{\partial t} &\approx \frac{1}{2}\sum_\alpha\Big(\int_{-\infty}^\infty e^{-i\omega_\alpha\tau}R_\alpha(\tau)\ d\tau\Big)\ (\hat{A}_\alpha\ \overline{\tilde{\rho}(t)}\ \hat{A}_\alpha^\dagger - \overline{\tilde{\rho}(t)}\ \hat{A}_\alpha^\dagger\hat{A}_\alpha + h.c.), \\ &= \sum_\alpha J_\alpha(\omega_\alpha)\ (\hat{A}_\alpha\ \overline{\tilde{\rho}(t)}\ \hat{A}_\alpha^\dagger - \frac{1}{2}\{\hat{A}_\alpha^\dagger\hat{A}_\alpha, \overline{\tilde{\rho}(t)}\}, \\ &= \sum_\alpha J_\alpha(\omega_\alpha)\ \hat{D}[A_\alpha][\ \overline{\tilde{\rho}(t)}\ ].\end{aligned} \tag{2.33}$$

Here, the cross correlation terms are neglected by assuming $R_{\alpha\beta}(\tau) = \delta_{\alpha\beta}R_\alpha(\tau)$. It is important to note that the semi-classical Redfild equation appears in the Lindbad form where each dissipative process $\hat{D}[A_\alpha][.]$ occurs at rate $J_\alpha(\omega_\alpha)$. This result will be used in Section 4.11 to analyze the dipolar coupling relaxation in the methyl group in the liquids phase [30]. It is remarkable that the quantum Redfield master equation in Equation (2.26) can also be written in the Lindbladian form in Section 2.4.1, and the only difference is the definition of the correlation function and the spectral density of noise that is replaced with

$$\begin{aligned}R_{\alpha\beta}(\tau) &= Tr_E[\hat{g}_\alpha(t)\hat{g}_\beta^\dagger(t+\tau)\rho_E], \\ J_{\alpha\beta}(\omega) &= \int_{-\infty}^\infty \langle\hat{g}_\alpha(t)\hat{g}_\beta^\dagger(t+\tau)\rangle\ e^{-i\omega t}d\tau.\end{aligned} \tag{2.34}$$

Here, $\hat{g}_\alpha(t)$ acts on the environment.

2.5 Postulate III: Quantum Measurement

The notion of quantum measurement and its interpretation has been a controversial subject [31]. One intuitive way of describing a quantum measurement is to treat it as an evolution process during which the experimental apparatus interacts with the the quantum system in order to *read* some information from that. As a result of this correlation, some statistical information about the system is obtained at the expense of *disturbing* the state of the system. However, modeling and characterizing the interaction between the system (micro) and the measurement apparatus (macro) is challenging, because, there are many inaccessible degrees of freedom. Finding a quantum model that provides a good description of evolution during the measurement, is an active field of research [32]. An operational alternative way of describing a quantum measurement is to focus on formulating the *effect* of a measurement regardless of the details of the evolution.

In the third postulate of quantum mechanics, the effect of a quantum measurement is described by a set of mathematical operators.

2.5.1 Ideal Measurement

In the simplest model of a quantum measurement, for every outcome m, a Positive Value Measure (PVM) operator Π_m is assigned to describe the *effect* of the measurement. PVM operators $\{\Pi_m\}$, are known as the *projective* or the *von Neumann* operators with properties $\Pi_m = \Pi_m^\dagger$ and $\Pi_m \Pi_n = \delta_{mn}\, \Pi_m$. According to the Born's rule, the probability of obtaining an outcome m is

$$p(m) = Tr[\Pi_m\, \rho]. \tag{2.35}$$

For example, in Stern-Gerlach experiment on spins, when a beam of spin half particles pass through an inhomogeneous magnetic field, it deflects into the "up" beam and the "down" beam. Correspondingly, the measurement operators are $\Pi_\uparrow = |\uparrow\rangle\langle\uparrow|$ and $\Pi_\downarrow = |\downarrow\rangle\langle\downarrow|$ which are orthogonal projective operators associated with the outcome "up" and "down".

As soon as an outcome m_0 is recorded, the assigned density matrix of the quantum system is *disturbed* and must be updated. According to the *Lüders* rule, those post selected events with outcome m_0 are associated with the *updated* density matrix

$$\rho^{|m_0} = \frac{\Pi_{m_0}\, \rho\, \Pi_{m_0}}{p(m_0)}. \tag{2.36}$$

The factor $1/p(m_0)$ ensures that the post-selected state is normalized.

There are two remarks about PVM measurements: First, the well known and yet bizarre concept of *collapsing* the wavefunction that has been extensively used in literatures refers to this state update rule where a PVM measurement *projects* the density matrix to a particular subspace that is associated with m_0. This concludes that a PVM measurement is a *destructive* measurement; Second, since PVM operators are orthogonal to each other, the measurement outcomes have *distinct* values. Therefore, a projective measurement is reproducible in the sense that two subsequent identical PVM measurements result in identical outcomes.

2.5.2 Generalized Measurement

In *generalized* measurement, the *effect* of any quantum measurement is described by a Positive Operator Valued Measure (POVM) denoted by E_m. The analog to the Born's rule is [20, 26],

$$p(m) = Tr[E_m\,\rho]. \tag{2.37}$$

Since the probabilities must be positive and add up to one, $E_m > 0$ and $\sum_m E_m = \mathbb{1}$. Projective measurement is a special case of POVM measurements.

Theorem 2.14. *(**Neumark's theorem** [33]): For any POVM operator E_m^A acting on $\rho_A \in \Gamma(\mathscr{H}_A)$, there exist a PVM operator Π_m^{AB} acting on a larger Hilbert space $\mathscr{H}_{AB}$ with $\rho_{AB} = \rho_A \otimes |\phi\rangle\langle\phi|_B$ such that*

$$p(m) = Tr_{AB}[\Pi_m^{AB}\ \rho_A \otimes |\phi\rangle\langle\phi|_B] = Tr_A[E_m^A\,\rho_A]. \tag{2.38}$$

To understand the concept of a POVM measurement and its realization via the Numark's theorem, let us provide a physical example. In a quantum measurement, the system A with an initial state ρ_A interacts with an experimental apparatus B with an initial state $\rho_B = |0\rangle\langle 0|_B$. We treat AB as a composite closed system that evolves under a unitary U_{AB} during the measurement time. Because, the user reads the outcomes from the apparatus alone, for a set of distinct measurement outcomes, $\{m_1, m_2, ..., m_n\}$, we associate a set of PVM operators, $\{\Pi_m^B = |m\rangle\langle m|\}$ that act on B alone. Considering the Born's rule and the Neumark's theorem, we obtain

$$\begin{aligned} p(m) &= Tr_{AB}[\ (\mathbb{1}_A \otimes \Pi_m^B)\ U(\rho_A \otimes \rho_B)U^\dagger], \\ &= \sum_a \langle a|\ \langle m|U_{AB}|0\rangle\ \rho_A\ \langle 0|U_{AB}^\dagger|m\rangle\ |a\rangle, \\ &= \sum_a \langle a|\mathscr{M}_m\,\rho_A\,\mathscr{M}_m^\dagger|a\rangle, \\ &= Tr_A[\mathscr{M}_m^\dagger\mathscr{M}_m\,\rho_A], \end{aligned} \tag{2.39}$$

where $\mathscr{M}_m := \langle m|U_{AB}|0\rangle$ is an effective operator acting on A that represents the reduced effect of the interaction between the system and the measurement apparatus. In this example, the POVM operators are $\{E_m = \mathscr{M}_m^\dagger \mathscr{M}_m\}$ and they are positive and $\sum_m E_m = \mathbb{1}_A$. The updated density matrix associated with outcome m_0, is

$$\rho^{|m_0} = \frac{k_{m_0}\ \rho\ k_{m_0}^\dagger}{p(m_0)}. \tag{2.40}$$

Despite PVM measurements, the state update rule is not unique for POVM measurements. In the above particular example, even if we assume that the interaction model is known (U_{AB} is known), the explicit form of $\mathscr{M}_m = \langle m|U|0\rangle$ is not unique, because, there is a freedom in the initial state of the apparatus. Furthermore, for a known POVM E_m, there is a freedom in its decomposition to $E_m = \mathscr{M}_m^\dagger \mathscr{M}_m$. For example, one could do it in a trivial manner by choosing $\mathscr{M}_m := \sqrt{E_m}$ [20]. Therefore, in case of the generalized measurements, the state update rule is not unique.

2.5.3 Quantum Measurement in NMR

In a typical NMR set up, there is a large static field along the z axis and an NMR coil in the transverse plane which generates and/or detects oscillating fields. In a classical approach, a time-dependent transverse magnetization $\vec{M}(t)$, induces a flux in the NMR coil which is detectable. The induced electro motive force is

$$emf = -\frac{d}{dt}\int \hat{B}_1.\vec{M}(t)\ d\Omega. \tag{2.41}$$

Here, $\hat{B}_1$ is the RF field direction and the integration is over the coil volume. Thus, the voltage generated in the NMR coil is proportional to the collective magnetization in the transverse plane. In a semi-classical approach, the NMR detection coil is still treated classically but the spin magnetization is treated quantum mechanically. $\vec{M}(t)$ is the expectation value of the transverse components of the collective spin angular momentum operators; $M_x(t) = \hbar\gamma\ Tr[\mathbf{S}_x\ \rho(t)]$ and $M_y(t) = \hbar\gamma\ Tr[\mathbf{S}_y\ \rho(t)]$. Therefore, to formulate the NMR signal, it is required to compute the evolution of the density matrix $\rho(t)$. In a full quantum mechanical approach, both the spin system and the NMR detection coil are treated quantum mechanically and there has been a few studies in this regards, [34]. In the following discussion we consider the semi-classical approach that is commonly used in the NMR textbooks, [28, 29, 35].

A very simple yet informative example is the NMR signal of N identical non-interacting spins at field $B_0\ \hat{z}$ and at temperature T, whose density matrix is given by $\frac{(\mathbb{1}+\varepsilon_0\ \sigma_z)}{2}^{\otimes N}$ in Section 2.2.2. In the absence of any relaxation and/or decoherence, a collective $\frac{\pi}{2}$ rotation around the $-y$ axis

followed by a free precession at rate ω_0, evolves this spin ensemble to

$$\rho_{\text{ensm}}(t) = \frac{1}{2}(\mathbb{1} + \varepsilon_0 \ (\cos\omega_0 t \ \sigma_x + \sin\omega_0 t \ \sigma_y))^{\otimes N} \tag{2.42}$$

The above ensemble evolution is obtained by replacing the individual spin's evolution from Section 2.3.1. A *continuous non-disturbing* measurement of this spin ensemble results in

$$\begin{aligned} M_x(t) &= \hbar\gamma \, Tr[\mathbf{S}_x \, \rho_{\text{ensm}}(t)] \\ &= \frac{N\hbar\gamma}{2}\varepsilon_0 \ \cos\omega_0 t \end{aligned} \tag{2.43}$$

A similar expression is obtained for the measurement in the y direction. The average of the magnetization in the transverse plane (M_x and/or M_y), is commonly reported as the NMR signal. This involves some implicit assumptions and approximations that we try to clarify in the following. For simplicity, we refer to the x component as the transverse magnetization, because the argument is similar for the y component.

Consider a hypothetical experiment where we are given n identical copies of a single spin system with $\rho_{\text{sing}} = \frac{1}{2}(\mathbb{1} + \varepsilon_0 \ \sigma_x)$. Suppose we make a projective measurement on each spin with PVM operators $\Pi \in \{|+\rangle\langle+|, |-\rangle\langle-|\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \pm |\downarrow\rangle)$. The average value of these identical measurements in the limit of large n is

$$\mu_x(0) = \hbar\gamma \, \langle S_x\rangle_{t=0} = \sum_s \ s \ Tr_s[\ \sigma_x \ \rho_{\text{sing}}] = \frac{\hbar\gamma}{2}\varepsilon_0. \tag{2.44}$$

Here, $s \in \{\frac{\hbar\gamma}{2}, -\frac{\hbar\gamma}{2}\}$ is the single spin outcome. We repeat this hypothetical experiment for another set of initial states

$$\rho_{\text{sing}}(\delta t) = \frac{1}{2}(\mathbb{1} + \varepsilon_0 \ (\cos\omega_0\delta t \ \sigma_x + \sin\omega_0\delta t \ \sigma_y). \tag{2.45}$$

The average value of this second round of identical measurements is $\mu_x(\delta t) = \frac{\hbar\gamma}{2}\varepsilon_0 \ \cos\omega_0\delta t$. If we keep doing this for all instances of time, we obtain a *continuous* signal which is the average of the transverse magnetization of a single spin that varies by time,

$$\mu_x(t) = \frac{\hbar\gamma}{2}\varepsilon_0 \ \cos\omega_0 t. \tag{2.46}$$

A practical way of computing the above average value is $\mu_x(t) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} s_i$, in which $\{s_1, s_2, ..., s_n\}$ is a string of outcomes generated by the identical PVM measurements on n identical copies of $\rho_{\text{sing}}(t)$.

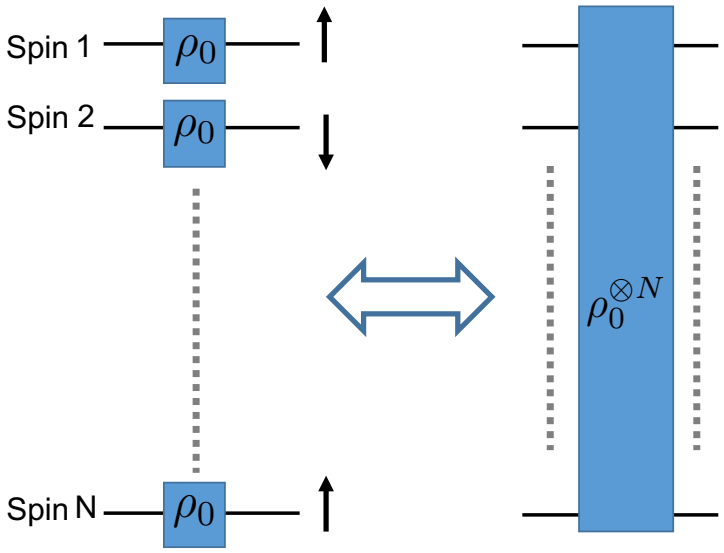

Figure 2.2: An NMR single shot measurement of an ensemble of N non-interacting spins is not equivalent to N times the average value of individual spins' measurements. But, for a very large ensemble it is an approximation.

By comparison between the above hypothetical experiment of single spin measurement in Equation (2.46) with the measurement of an ensemble of non-interaction identical spins in Section 2.5.3, we conclude that $M_x(t) = N\mu_x(t)$. This relation between the collective signal and the individual spins' signal sounds very trivial but the above hypothetical experiment clarifies two important implicit assumptions that are often made by considering $M_x(t)$ as the NMR signal: First, the generated signal at each instance of time, $M_x(t)/\mu_x(t)$, is the *average value* of the transverse magnetization not the outcome of a *single shot measurement*; Second, the measurements are *non-disturbing* and the state update rule is neglected[1]. Neglecting the state update rule is equivalent to having access to a *fresh copy* of $\rho_{\text{ensem}}(t)/\rho_{\text{sing}}(t)$ at each instance of time which hasn't been disturbed by the *history* of previous measurements. We would like to know up to which extend these implicit assumptions are valid to consider $M_x(t)$ as a good approximation of the NMR signal.

Consider a *single shot* ideal measurement of this ensemble of N non-interacting identical spins. The outcome is a sum of all individual spins' magnetization, i.e. $m_x = \sum_{j=1}^{N} s^{(j)}$ where

[1]Here, for the sake of argument, we consider a simple coherent evolution only. Coil back action or radiation damping is well studied [28].

$s^{(j)} \in \{\frac{\hbar\gamma}{2}, -\frac{\hbar\gamma}{2}\}$. Obviously, $m_x \neq N \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} s_i$, and so, a single shot measurement on an ensemble, in general, is not equal to the sum of the average value of the individual spins' measurement, i.e. $m_x \neq M_x$. However, often in NMR, we deal with a very large spin ensemble ($N \geq$ Avogadro number) and in that limit, it is a fair approximation to consider $m_x \approx M_x = N\mu_x$. This approximation of a single shot measurement of an ensemble vs an average value of individual spin measurement is demonstrated in Figure 2.2. We emphasize that there are times where describing the correct physics requires a collective spin model rather than individual spin picture. An example is the quantum spin fluctuation phenomenon that will be explained in Chapter 3. That chapter also elaborates on the importance of the state update rule which is normally neglected and provides a quantum description of spin noise in both the strong measurement and the weak measurement limits.

2.6 Mathematical Representations of CPTP Maps

In Section 2.4, the solution of a Markovian master equation was denoted by a linear CPTP map $\mathscr{E} \in \mathbf{L}(\mathscr{H})$ which is more general than a unitary operator. The linear map $\mathscr{E}$ is a quantum operation that describes a snapshot of time evolution of an open quantum system and has other familiar names such as *quantum map*, *quantum channel* or *quantum transformation*. As mentioned before, $\mathscr{E} : \mathbf{L}(\mathscr{H}) \to \mathbf{L}(\mathscr{H})$ describes a physical process where it transforms a density matrix to a density matrix, and therefore, it must be a Completely Positive Trace Preserving map (CPTP). Mathematically, there are several equivalent types of representation of a CPTP map and in this section we briefly review some of those representations, [36].

2.6.1 System-Environment Representation

The most intuitive way of describing the evolution of an open quantum system is the system-environment model. In this model, the principle system S, interacts with another system named environment E, via a unitary operator U_{SE}. The reduced system dynamics is derived by taking a partial trace over the other environment,

$$\mathscr{E}[\rho_S] = Tr_E[(U_{SE}\ (\rho_S \otimes \rho_E)\ U_{SE}^{\dagger}]. \tag{2.47}$$

Here, ρ_E is the initial state of the environment and is assumed to be uncorrelated from the system of interest. Note that the space of environment here is a mathematical notion and its dimension needs to be at most d^2 [20]; therefore, when it comes to application of this model to a real

physical process, careful considerations must be taken because the system-environment model is not unique. This arises because one can find different real physical processes that all result in the same quantum map on the reduced system. The system-environment model is an application of *Stinespring Dilation* theorem [37], and it is common to call it as *Stinespring representation*.

2.6.2 Kraus Representation

An alternative mathematical description of $\mathscr{E}$ is the Kraus representation, given by the following theorem.

Theorem 2.15. *For any CPTP map $\mathscr{E} : \boldsymbol{L}(\mathscr{H}) \to \boldsymbol{L}(\mathscr{H})$, there exist a set of operators $\{K_i\}$, satisfying the condition $\sum_i K_i^\dagger K_i = \mathbb{1}$ such that*

$$\mathscr{E}[\rho] = \sum_i K_i \, \rho \, K_i^\dagger . \tag{2.48}$$

This is called Kraus representation [38] and $\{K_i\}$ are called Kraus operators. To clarify the Kraus representation, we elaborate on two examples of T_1 relaxation and T_2 dephasing processes which are well known processes in NMR.

In a pure T_1 process, any arbitrary spin system in a field B_0 and at temperature T, relaxes to the equilibrium state ρ_0 with Boltzmann polarization $\varepsilon_0 = \tanh[\frac{\hbar\gamma B_0}{2k_bT}]$. Mathematically, one can represent this relaxation process in terms of the following Kraus operators

$$\begin{aligned} K_1 &= \sqrt{\frac{(1+\varepsilon_0)}{2}} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, \qquad K_2 = \sqrt{\frac{(1+\varepsilon_0)}{2}} \begin{pmatrix} 0 & \sqrt{\lambda} \\ 0 & 0 \end{pmatrix}, \\ K_3 &= \sqrt{\frac{(1-\varepsilon_0)}{2}} \begin{pmatrix} \sqrt{1-\lambda} & 0 \\ 0 & 1 \end{pmatrix}, \qquad K_4 = \sqrt{\frac{(1-\varepsilon_0)}{2}} \begin{pmatrix} 0 & 0 \\ \sqrt{\lambda} & 0 \end{pmatrix}. \end{aligned} \tag{2.49}$$

Here, $\lambda = \frac{\delta t}{T_1}$ is the probability of transition between $|\uparrow\rangle \rightleftharpoons |\downarrow\rangle$ during the time interval δt. For short evolution, this set of Kraus operators transforms an arbitrary initial state $\rho_{in} = \begin{pmatrix} a & b \\ b^* & 1-a \end{pmatrix}$ to

$$\begin{aligned} \mathscr{E}_1[\rho_{in}] &= \sum_{i=1}^{4} K_i \, \rho_{in} \, K_i^\dagger \\ &= \begin{pmatrix} a(1-\lambda) + \frac{1+\varepsilon_0}{2} & b\sqrt{1-\lambda} \\ b^*\sqrt{1-\lambda} & (1-a)(1-\lambda) + \frac{1-\varepsilon_0}{2} \end{pmatrix}. \end{aligned} \tag{2.50}$$

For a long evolution, t can be discretized into smaller steps by $t = \lim_{n\to\infty} n\ \delta t$. Afterwards, the above Kraus operators are repeatedly applied on ρ_{in} for n time and ultimately

$$\lim_{n\to\infty} (\mathscr{E}_1[\rho_{in}])^n = \frac{1}{2}(\mathbb{1} + \varepsilon_0\sigma_z).$$

In the last part of the calculation, $\lim_{n\to\infty}(1-\lambda)^n = e^{-t/T_1}$ is replaced and in the limit of $t \to \infty$ this term vanishes. Note that a T_1-relaxation also induces a decoherence process that reduces the off-diagonal terms at the rate $\frac{1}{2T_1}$. The above mathematical Kraus operators describes T_1 relaxation towards the equilibrium state.

In a pure T_2 process, the off-diagonal terms of the density matrix are attenuated which leads to a loss of coherence for superposition states. Mathematically, one can represent this *decoherence* process, known as *dephasing* [20], in terms of the following Kraus operators

$$K_1 = \sqrt{1-\frac{\gamma}{2}}\,\mathbb{1}, \qquad K_2 = \sqrt{\frac{\gamma}{2}}\,\sigma_z. \tag{2.51}$$

Here, $\frac{\gamma}{2} = \frac{\delta t}{T_2}$ is the probability of decoherence during the time interval δt. For short evolution, this dephasing process transforms an arbitrary initial state ρ_{in} to

$$\mathscr{E}_2[\rho_{in}] = \begin{pmatrix} a & b\,(1-\gamma) \\ b^*\,(1-\gamma) & 1-a \end{pmatrix}. \tag{2.52}$$

Like before, for longer evolution time t, the above Kraus operators are repeatedly applied on ρ_{in} for n time and ultimately

$$\lim_{n\to\infty} (\mathscr{E}_2[\rho_{in}])^n = a\ |\uparrow\rangle\langle\uparrow| + (1-a)\ |\downarrow\rangle\langle\downarrow|.$$

The off-diagonal terms or the coherence terms are attenuated by $\lim_{n\to\infty}(1-\gamma)^n = e^{-t/T_2}$ and in the limit of $t \to \infty$ all coherences are lost and the off-diagonal terms vanishes.

The final remark about the Kraus representation is that the set of Kraus operator that describes a specific physical process is not unique. For example, a T_2 process can also be described by

$$K_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \qquad K_2 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\gamma} \end{pmatrix}. \tag{2.53}$$

2.6.3 Liouville-operator Representation

Consider the Markovian master equation in Equation (2.24). We re-write the master equation in a *Liouville space*, where all density matrices and quantum maps are *vectorized* according to Definition 2.10,

$$\frac{d\|\rho\rangle\!\rangle}{dt} = (\hat{\hat{G}}_H + \hat{\hat{G}}_{\mathscr{D}})\,\|\rho\rangle\!\rangle. \tag{2.54}$$

Here, the superoperators $\hat{\hat{G}}_H$ and $\hat{\hat{G}}_{\mathscr{D}}$ are the Liouville representations of the coherence evolution map $-i[H,.]$ and the dissipative evolution map $\hat{\mathscr{D}}[.]$ respectively. The double hat notation emphasizes that these superoperators are represented in the Liouville space. The above *vectorized* version of the master equation has a similar form to the Schrödinger equation for closed systems. Thus, its solution is

$$\|\rho(t)\rangle\!\rangle = \hat{\hat{S}}(t)\,\|\rho(0)\rangle\!\rangle \quad \text{with} \quad \hat{\hat{S}}(t) = \mathscr{T} e^{\int_0^t (\hat{\hat{G}}(t')\,dt'}, \tag{2.55}$$

in which $\mathscr{T}$ is the time-ordering operator, $\hat{\hat{G}}(t) = \hat{\hat{G}}_H(t) + \hat{\hat{G}}_{\mathscr{D}}(t)$ is the generator, and $\hat{\hat{S}}(t)$ is the Liouville-representation or the superoperator representation of the quantum evolution map $\mathscr{E}[\rho]$. In other words, $\hat{\hat{S}} : \|\rho\rangle\!\rangle \rightarrow \|\mathscr{E}[\rho]\rangle\!\rangle$, and hence,

$$\mathscr{E}[\rho]_{ij} = \sum_{\mu\nu} \hat{\hat{S}}_{ij,\nu\mu}\,\rho_{\mu\nu}. \tag{2.56}$$

If both the Hamiltonian and the dissipator are time-independent, the generator $\hat{\hat{G}}$ becomes time-independent, and thus, $\hat{\hat{S}}(t)$ has a simple exponential form $\hat{\hat{S}}(t) = e^{\hat{\hat{G}}\,t}$. In that case, it has been shown that the real part of all eigenvalues of $\hat{\hat{G}}$ must be non-positive with at least one zero eigenvalue [39]. Otherwise, when $t \rightarrow \infty$, the superoperator $\hat{\hat{S}}$ transforms a density matrix to a non-physical state.

2.6.4 Choi Matrix Representation

The Choi matrix representation makes a duality between quantum channels and quantum states. This is an application of Choi-Jamiolkowski isomorphism which relates linear maps acting on $\mathbf{L}(\mathscr{H}_A)$ and the density operators in an extended Hilbert space, $\mathbf{L}(\mathscr{H}_{AB})$ [40, 41].

Definition 2.16. Any CPTP map $\mathscr{E} : \mathbf{L}(\mathscr{H}_{A'}) \rightarrow \mathbf{L}(\mathscr{H}_B)$ that acts on half of a Bell state $|\Phi^+\rangle_{AA'}$, is related to a unique density matrix in a larger Hilbert space, $\rho_{AB} \in \Gamma(\mathscr{H}_{AB})$ with

$$\rho_{AB} = (\mathbb{1} \otimes \mathscr{E})|\Phi^+\rangle\langle\Phi^+|_{AA'}. \tag{2.57}$$

Reversely, for known $\rho_{AB} \geq 0$, one can characterize the CPTP map $\mathscr{E}[\rho]$ via

$$\mathscr{E}[\rho] = Tr[(\rho^T \otimes \mathbb{1})\rho_{AB}] \tag{2.58}$$

The Choi matrix representation is a very useful tool in characterizing a noisy quantum communication channel and is widely used in quantum information theory.

Chapter 3

Quantum Model Of Spin Noise

Any ensemble of quantum particles exhibits statistical fluctuations known as spin noise. In this section, we provide a description of spin noise in the language of open quantum systems.

3.1 Introduction

Spin noise is a signal due to the quantum fluctuations of an ensemble. This phenomenon has been studied experimentally and theoretically, [42–45]. Here, we describe an open quantum system approach that provides a simple description of spin noise. This analysis of spin noise may lead to a clearer understanding of foundational concepts in quantum mechanics such as measurement and fluctuation. The experimental observation of spin noise also finds application in NMR when the sample has a small number of spins, and/ or a very long relaxation time.

Bloch in his original paper in 1946 predicted that even in the absence of any external magnetic field there would still exist a "*resultant moment due to statistically incomplete cancellation*" with a magnitude that scales with the square root of the number of spins [42]. Sleator & Hahn [43] observed spin noise in low temperature NMR using a high Q superconducting quantum interference device (SQUID resonator). In 1989, Ernst & McCoy [44] observed spin noise at room temperature in a high sensitive liquid state NMR probe. Similarly, Gueron & Leroy [45] observed spin noise in a sample of water.

Spin noise is a signature of any ensemble of quantum systems. There have been several other observations of spin noise effects including via magnetic resonance force microscopy, spin imaging, quantum dots and optics, [46–51]. Additionally, Holt & Ginsberg and Tropp, [34, 52], have given a quantum description of its origin.

For spin half particles the amplitude of the spin noise fluctuation grows as the square root of the number of spins, exists in all directions on the Bloch sphere and has a characteristic correlation time resulting from the internal Hamiltonian and the relaxation times.

There are two cases where the spin noise signal is greater than the thermal polarization signal: a small sample and a smple with long relaxation time. At equilibrium, the Boltzmann polarization is $M_0 \sim N\frac{\hbar\gamma}{2}\tanh[\frac{\hbar\gamma B_0}{kT}]$ where γ is the gyromagnetic ratio of the spin. The most efficient detection for a repeated measurement of a free induction decay is the Ernst angle experiment with nutation angle β, set as $\cos\beta = \exp(-\tau/T_1)$ where τ is the recycle time [29]. This results in a steady state magnetization of $M_0\sqrt{(1-\cos\beta)/(1+\cos\beta)}$ and one can compare it to the spin noise ($\sim \sqrt{N}\frac{\hbar\gamma}{2}$) and conclude that for a small sample, $N < (\sqrt{(1-\cos\beta)/(1+\cos\beta)}\varepsilon_0)^{-2}$ and/ or a very long relaxation time, $T_1 > \tau(\ln[\cos^{-1}[\frac{1-N\varepsilon_0^2}{1+N\varepsilon_0^2}]])^{-1}$ where $\varepsilon_0 = \tanh[\frac{\hbar\gamma B_0}{kT}]$, the spin noise is greater than the thermal polarization.

Here, we apply the theory of open quantum systems to describe the origin and the correlation function of the spin noise signal. The analysis shows that we can model spin noise by separately modelling the quantum measurement and the quantum evolution of the spin system. First, in Section 3.2, we outline the general approach and introduce the model. Then, in Section 3.3, we gain physical insight about spin noise by exploring the case of a totally mixed input state, an ideal strong measurement and a depolarizing quantum map. This simple yet concrete example allows us to introduce all of the tools we will need. Following this, we investigate the case of an arbitrary quantum evolution acting on a non-interacting ensemble of spins. Finally, we study the effect of weak measurement on the system.

3.2 Open Quantum System Model

In an NMR measurement, an ensemble of spins (sample) is coupled to a bath (environment) and a detection coil (cavity). The total Hamiltonian of this system is

$$H_{\text{tot}} = H_s + H_B + H_{Bs} + H_c + H_{sc}, \tag{3.1}$$

where the first three terms are the spins, the bath and the spin-bath interaction Hamiltonians, and the last two terms are the cavity interaction Hamiltonians. We are interested in the dynamics of the spin ensemble alone. Since it is interacting with a bath and a measurement apparatus, an open quantum system approach is convenient. In what follows, we describe an effective quantum evolution map (a time snapshot of a propagator) on the N spin ensemble when either just the bath or just the cavity is considered. Then, we combine these to describe the full evolution.

Consider an initial state with no spins/bath correlations. Given the time dependent Hamiltonian $H_s + H_B + H_{Bs}(t)$, this bipartite system evolves under the unitary operator which is the solution of Schrödinger's equation for a closed system [29],

$$\begin{aligned} \rho_{Bs}(t) &= U_{Bs}(t)(\rho_B(0) \otimes \rho_s(0))U_{Bs}^{\dagger}(t), \\ \text{where} & \\ U_{Bs}(t) &= \mathscr{T} e^{-i\int_0^t (H_s + H_B + H_{Bs}(t))\, dt'}. \end{aligned} \tag{3.2}$$

In order to find the reduced evolution operator on the spin ensemble, one can use the system-environment representation (Figure 3.1) and obtain

$$\begin{aligned} \rho_s(t) &= Tr_B[\rho_{Bs}(t)] \\ &= Tr_B[U_{Bs}(t)(\rho_B(0) \otimes \rho_s(0))U_{Bs}^{\dagger}(t)] \\ &= \Lambda_t[\rho_s(0)]. \end{aligned} \tag{3.3}$$

The quantum evolution map Λ_t, is not generally a unitary evolution, as it was explained in Section 2.4. This is the distinction between a closed and an open system. In fact, since Λ_t maps a density matrix to a density matrix for an initially uncorrelated state of the spin and the bath, it is completely positive and trace preserving (CPTP). According to Section 2.4, if the bath interaction is Markovian, the dynamics of the spin ensemble as an open quantum system is govern by [29] and [26]

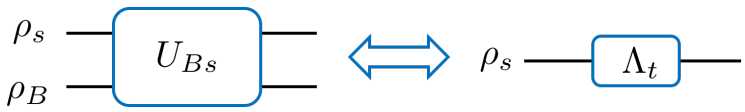

Figure 3.1: The reduced time evolution operator (CPTP map) on an ensemble of spins coupled to a bath.

$$\frac{\partial \rho_s(t)}{\partial t} = -i[H_s, \rho_s(t)] + \hat{\mathscr{D}}\,[\rho_s(t)] \tag{3.4}$$

where the evolution depends on both the coherent evolution $-i[H_s, \cdot]$, and the dissipator $\hat{\mathscr{D}}[\cdot]$, which describe the effective result of coupling to the bath. This term leads to decoherence or relaxation and drives the system towards its equilibrium state. The dissipator is derived in [29] and [26] via a quantum mechanical approach that we briefly review. The interaction Hamiltonian can be written as

$$H_{sB} = \sum_{\alpha} \hat{B}_{\alpha}(t) \otimes \hat{A}_{\alpha}$$

where the operators $\hat{A}_\alpha$ are acting on the spin system and the operators $\hat{B}_\alpha(t)$ are fluctuating randomly and are acting on the bath system. One can find the bath time correlation function

$$R_{\alpha\beta}(\tau) = \overline{\hat{B}_\alpha(t)\hat{B}^\dagger_\beta(t+\tau)} \tag{3.5}$$

from which the spectral density of noise is known, $J_{\alpha\beta}(\omega) = \int d\tau\ e^{-i\omega t}\ R_{\alpha\beta}(\tau)$. Then, under some assumptions [29] & [26], one can find the relaxation dissipator

$$\hat{\mathscr{D}}\ [\rho_s(t)] = \sum_\alpha J_\alpha(\omega_\alpha)\ (\hat{A}_\alpha\ \rho_s(t)A^\dagger_\alpha - \frac{1}{2}\{A^\dagger_\alpha A_\alpha,\ \rho_s(t)\})$$

where $\hat{A}_\alpha$ satisfies $[H_s,\hat{A}_\alpha] = \omega_\alpha\ \hat{A}_\alpha$. Given this last relation for $\hat{\mathscr{D}}[\rho_s]$, the solution of the master equation in Equation 3.4, is the same as the quantum evolution map defined in Equation 3.3 under the Markovian interaction. Interestingly, the above dissipator operator that was derived based on quantum mechanical approach is very similar to the semi-classical approach derived in Section 2.4.1. The only difference is the correlation function when the bath is treated classically, $R(\tau) = \overline{g(t)g^*(t)(t+\tau)}$, versus when the bath is treated quantumly, $R(\tau) = \overline{\hat{B}(t)\hat{B}^\dagger(t+\tau)}$.

3.2.1 Cavity Interaction

We would like to find an effective map on the N spin system which is purely due to coupling to the measurement apparatus. Consider those terms of the Hamiltonian in Equation 3.1 that involves the detection coil only, i.e., $H_c + H_{sc}$. This system evolves unitarily

$$\rho_{sc}(t) = U_{sc}(\rho_s \otimes |\psi\rangle\langle\psi|_c)U^\dagger_{sc},$$

where $U_{sc} = \exp(-i(H_c + H_{sc})\ t)$.

For our analysis, the cavity does not distinguish between spins and the spins only couple to a single mode. This is described by the Tavis-Cumming Hamiltonian [53]

$$H_c + H_{sc} = \omega_c\ \hat{a}^\dagger\hat{a} + g\ \mathbf{S}_x(\hat{a} + \hat{a}^\dagger).$$

Here, $\mathbf{S}_x = \sum_{i=1}^{N} S_x^{(i)}$ is the x component of the total spin angular momentum, and $\hat{a}$ and $\hat{a}^\dagger$ are the ladder operators. According to this model, the detection coil does not distinguish spins and in a measurement, the net magnetization of the whole ensemble is recorded, given by $m = \sum_{i=1}^{N} s^{(i)}$

with $s \in \{+\frac{1}{2}, -\frac{1}{2}\}$[1]. Thus, a measurement leaves the spin ensemble in a totally symmetric submanifold with net magnetization m. To see the effect of measurement explicitly, we note that the cavity is coupled to additional degrees of freedom that produce the observed measured outcomes (e.g, electronics). Effectively, the spin system couples to the measurement device (c') via the cavity interactions and once the measurement is completed the cavity is left in its initial state. This allows us to drop the cavity from the model. If the detection has an accuracy of one single spin flip, the possible measured outcomes are $m \in \{-\frac{N}{2}, -\frac{N}{2}+1, ..., \frac{N}{2}\}$ and correspondingly the measurement device Hilbert space is spanned by an orthonormal basis $\{|m\rangle\}$. For the evolved state $\rho_{sc'}(t)$, the Numark theorem leads to

$$\begin{aligned} Tr_{c'}[\rho_{sc'}(t)] &= Tr_{c'}[U_{sc'}\ (\rho_s(0) \otimes |\psi\rangle\langle\psi|_{c'})\ U_{sc'}^{\dagger}] \\ \rho_s(t) &= \sum_m \langle m|U_{sc'}|\psi\rangle_{c'}\ \rho_s(0)\ \langle m|U_{sc'}|\psi\rangle_{c'}^{\dagger} \\ &= \sum_m \mathscr{M}_m\ \rho_s(0)\ \mathscr{M}_m^{\dagger} \end{aligned} \tag{3.6}$$

where $\mathscr{M}_m = \langle m|U_{sc'}|\psi\rangle$ is defined as the measurement operator assigned to the measurement outcome m. According to Equation 3.6, the effect of the interaction with the detection coil appears as an effective quantum map $\mathscr{E}[\rho] = \sum_m \mathscr{M}_m\ \rho_s\ \mathscr{M}_m^{\dagger}$ on the spin ensemble. It is easy to check that $\mathscr{E}[\rho]$ is also a CPTP map and hence, $\sum_m \mathscr{M}_m^{\dagger}\mathscr{M}_m = \mathbb{1}$.

Notice that we considered an initial pure state $|\psi\rangle$ for the measurement device. One can generalize this argument for any initial mixed state $\rho_c(0)$, because it can be written as a convex combination of pure states and all of the maps in the presented model are linear.

In a quantum measurement there is a trade off between the amount of information obtained and the amount of disturbance introduced in the system. Say the detection coil measures the classical value m_0, then, the spin ensemble's state conditioned on the knowledge m_0 is updated to [20]

$$\rho^{|m_0} = \frac{\mathscr{M}_{m_0}\ \rho_s\ \mathscr{M}_{m_0}^{\dagger}}{p(m_0)}$$

where $p(m_0) = Tr[\mathscr{M}_{m_0}^{\dagger}\mathscr{M}_{m_0}\ \rho_s]$ is the probability that such an event occurs. In the case of a strong measurement, the ensemble magnetization m_0, is known with certainty. Therefore, the spin ensemble density matrix collapses (maximal disturbance) to the $m = m_0$ manifold only, and if we make a second measurement immediately afterwards, the outcome m_0 is reproduced. In other words, the conditional probability distribution of the second measurement is a delta

[1] From now on, we skip the constant coefficient $\hbar\gamma$ any time we mention the magnetization.

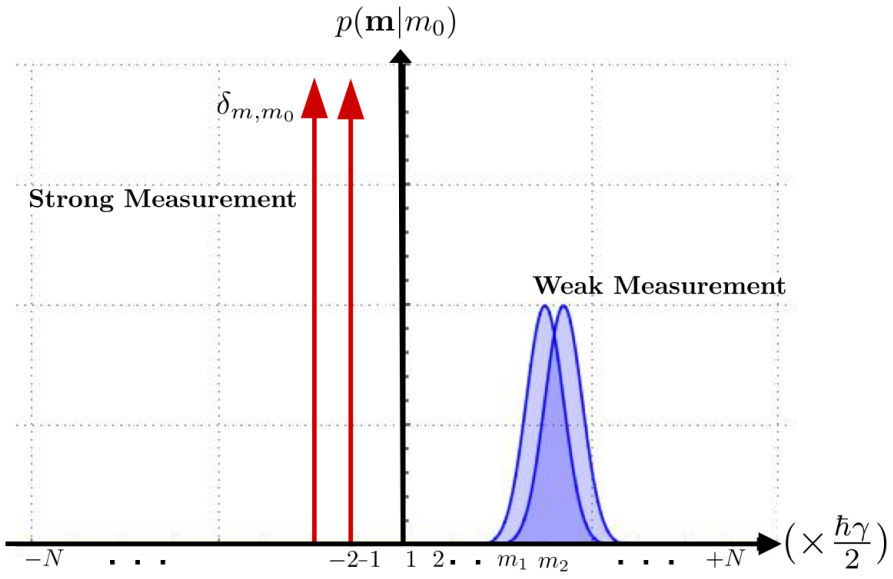

Figure 3.2: The conditional probability distribution of a strong measurement and a weak measurement are compared. In a strong measurement, the updated density matrix collapses sharply to the submanifold m_0 and this leads to a delta function distribution (red). Whereas, in a weak measurement, the density matrix is less disturbed and it collapses to an area centered at m_0. As a result, the corresponding probability distribution has a finite width (blue). The horizontal axis is in $\frac{\hbar\gamma}{2}$ unit and represents the net magnetization of the ensemble.

function, i.e, $p(\mathbf{m} \mid m_0) = \delta_{m,m_0}$. In the case of a weak measurement, the measurement apparatus is *less precise* and the spin ensemble state collapses not only to the $m = m_0$ manifold but also to the other neighbouring manifolds, $m \neq m_0$. So, if we immediately make another measurement, the outcome m_0 may not be reproduced. In other words, the conditional probability distribution $p(\mathbf{m} \mid m_0)$ could be a distribution function with mean value m_0 and a width w which is in inverse relation with the accuracy of the measurement device (Figure 3.2). We will provide a more detailed model of a strong and a weak measurement in Section 3.3 and Section 3.4.

3.2.2 N Spins Coupled to the Bath and the Cavity

So far, we have considered the effect of coupling to the measurement apparatus and the reduced quantum evolution map on the spin ensemble as two independent processes. However, in an NMR measurement these two processes occur simultaneously. Hence,

$$U_{Bsc}(T) = \mathscr{T} e^{-i\int_0^T H_{\text{tot}}(t')\,dt'}.$$

The various contributions of H_{tot} in Equation 3.1 do not in general commute at all times, and so, the formal solution is not practically helpful. One can discretize the total evolution time $T = n\,t$, in which t is small enough to allow a first order approximation. Then, for a short time evolution t, the first order of the Magnus expansion [22] is

$$\begin{aligned} U_{Bsc}(t) &\approx e^{-i\int_0^t (H_s + H_B + H_{Bs}(t'))dt} e^{-i(H_c+H_{sc})t}, \\ &= U_{sc}(t) U_{Bs}(t). \end{aligned} \tag{3.7}$$

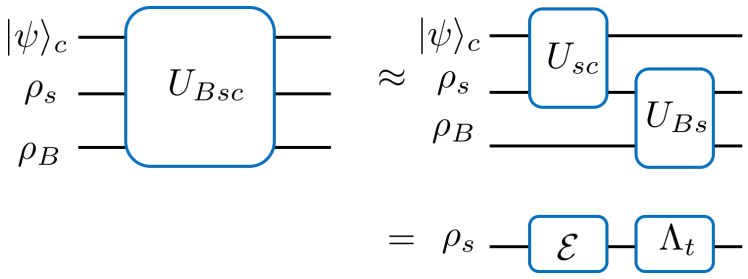

Figure 3.3: A first order approximation of time evolution of a bath-spin ensemble-cavity system is presented.

For example, in the case of $H_s = \omega_0\,\mathbf{S}_z$ and the Tavis-cumming model for interaction with the cavity, this approximation is valid if $t \ll \frac{1}{\sqrt{\omega_0}\,g}$. In this first order approximation, the effective quantum evolution map for the short time period t on the spin ensemble is

$$\begin{aligned} \rho_s(t) &= Tr_{Bc}[\, U_{Bsc}\, \rho_{Bsc}(0)\, U_{Bsc}^{\dagger}\,] \\ &\approx Tr_{Bc}[\, (U_{Bs}U_{sc})\, \rho_{Bsc}(0)\, (U_{Bs}U_{sc})^{\dagger}\,] \\ &= \Lambda_t[\, \mathscr{E}[\rho_s(0)]\,] \end{aligned} \tag{3.8}$$

where $\rho_{Bsc}(0) = \rho_B(0) \otimes \rho_s(0) \otimes |\psi\rangle\langle\psi|_c$. Therefore, a quantum evolution map on the spin ensemble, can be approximated by a sequence of measurement-evolution processes as schematically is shown in Figure 3.4.

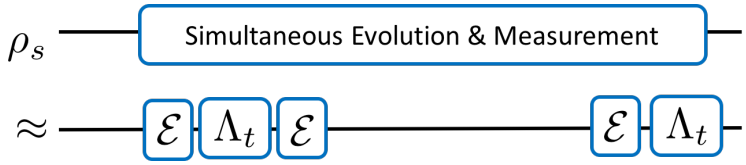

Figure 3.4: The effective time evolution operator on a spin ensemble is approximated by a sequence of measurement-evolution processes.

In the following sections, we apply this model to the examples of both strong and weak measurements under the evolution of a collective depolarizing map or any arbitrary CPTP map on individual spins. In each cases, we find the spin noise and its correlation function.

3.3 Strong Measurement Model

Suppose we have N identical spin half particles and we have no information about their spin orientation. So, at $t = 0$, the density matrix $\rho_0 = \frac{\mathbb{1}}{2^N}$ describes "our knowledge" about the system which is maximal ignorance. Now, according to the model presented in previous section, we make a series of strong measurements on the system by which we obtain information about the collective magnetization, $\mathbf{m}$[2]. Between two subsequent measurements, there is a time interval δt during which the system evolves under a quantum evolution map $\Lambda_{\delta t}$.

Without loss of generality, we assume the collective measurements are along the z axis. Of course, NMR detection is in the $x-y$ plane, but, for this analysis the direction is of no importance. At $t = t_n$, the recorded data $\mathbf{m}(t_n) = m_n$, is the eigenvalue of the z component of the total spin angular momentum, $\mathbf{S}_z$. This choice of collective measurement is not the common one in NMR, usually $N\langle S_z\rangle$ is used as the ensemble signal. However, in order to see the spin noise effects, one needs to keep track of what has been learned about the ensemble in each measurement rather than just the mean value. Therefore we do the analysis in the total angular momentum space. This has been used before [54].

The action of a strong measurement is described by a set of projection valued measure (PVM)

[2]To clarify the notation $\mathbf{m}$ is a random variable with domain $[-\frac{N}{2}, \frac{N}{2}]$ but m is a specific value.

operators $\{\mathscr{M}_m\}$ that we denoted by $\mathscr{M}_m = \Pi_m$ and are given by

$$\begin{aligned} \mathbf{S}_z &= \sum_m m\, \Pi_m \\ \Pi_m &\equiv \sum_{j=|m|}^{N/2} \sum_{d=1}^{A_j} |j,m,d\rangle\langle j,m,d|. \end{aligned} \tag{3.9}$$

where $\hbar = 1$. Here, $|j,m,a\rangle$ are degenerate eigenstates of the total spin angular momentum $\vec{\mathbf{S}} = \sum_{i=1}^{N} \vec{S}^{(i)}$ as well as its z component $\mathbf{S}_z$ operator. For N spin half particles, $j = j_0, j_0+1, ..., N/2$ where $j_0 = 0$ $(1/2)$ if N is even (odd). For each total spin angular momentum's eigenvalue, j, the collective magnetization in the z direction is $m = -j, j+1, ..., j$, and, the state degeneracy label is $d = 1,2,...,A_j$ where $A_j = \begin{pmatrix} N \\ \frac{N}{2}+j \end{pmatrix} - \begin{pmatrix} N \\ \frac{N}{2}+j+1 \end{pmatrix}$[18]. These eigenstates span the whole Hilbert space and form a basis for an ensemble of spins. It is common to consider j as the principle quantum number and, m as the second quantum number. However, mathematically it is equivalent to consider m as the principle number, $m \in \{-N/2, -N/2+1, ..., N/2\}$ and $|m| \leq j \leq N/2$ as the second quantum number which is the case in our notation. Note, by this definition, $\{\Pi_m\}$ satisfies the conditions of Projective Value Measure (PVM) operators, i.e, $\Pi_m.\Pi_n = \delta_{mn}\, \Pi_m$ and $\sum_m \Pi_m = \mathbb{1}$. An example of a strong measurement on a single spin is Stern-Gerlach experiment where the measurement operators are $\Pi_+ = |\uparrow\rangle\langle\uparrow|$ and $\Pi_- = |\downarrow\rangle\langle\downarrow|$ which are orthogonal projective operators corresponding to the outcome "up" and "down". Here, Π_m are the generalized form for an N spin projective measurement when the detection coil has the precision of one single spin.

The first measurement at t_1, results in outcome $m_1 \in [-\frac{N}{2}, \frac{N}{2}]$ which occurs with probability $p(m_1;t_1)$. This probability is a binomial (semi-Gaussian) distribution with zero mean and $\sqrt{N}$ standard deviation, because

$$\begin{aligned} p(\mathbf{m} = m_1;t_1) &= Tr[\Pi_{m_1}\rho_0] = \frac{Tr[\Pi_{m_1}]}{2^N} \\ \mathbb{E}[\mathbf{m};t_1] &= Tr[\mathbf{S}_z\rho_0] = 0 \\ \sigma[\mathbf{m};t_1] &= \sqrt{Tr[\mathbf{S}_z^2\rho_0] - (Tr[\mathbf{S}_z\rho_0])^2} = \frac{1}{2}\sqrt{N} \end{aligned} \tag{3.10}$$

This result matches what we intuitively expect. Each spin has magnetization $s^{(i)} \in \{+\frac{1}{2}, -\frac{1}{2}\}$, and, in each measurement shot, we take N samples from a distribution $p(s)$ with a width of $\frac{1}{2}$. Therefore, according to the central limit theorem, the collective magnetization $m = \sum_{i=1}^{N} s^{(i)}$ itself

is a random variable whose distribution is Gaussian with width of $\frac{\sqrt{N}}{2}$. Because the spins are indistinguishable, $Tr[\Pi_m]$ counts the number of configurations that all result in m_1 net magnetization and therefore $p(\mathbf{m};t_1)$ is a binomial distribution.

Once we learn the system, we must update its density matrix according to "our knowledge" of the outcome. Given the outcome m_1, the state update rule [20] dictates that

$$\rho^{|\mathbf{m}=m_1} = \frac{\Pi_{m_1}\,\rho_0\,\Pi_{m_1}}{p(m_1;t_1)} = \frac{\Pi_{m_1}}{Tr[\Pi_{m_1}]}. \tag{3.11}$$

The state in Equation 3.11 evolves under a quantum map Λ during the time interval δt after which the next measurement takes place. As an example, we consider a collective depolarizing map where with probability $(1-\lambda) = \exp[-\delta t/T]$ the quantum state is preserved and with probability λ it turns to a fully mixed state. The characteristic time T is a function of the depolarizing strength. Physically, a depolarizing map could be a result of a relaxation process in the system and mathematically is given by

$$\Lambda[\rho] = (1-\lambda)\,\rho + \lambda\,\frac{\mathbb{1}}{2^N}. \tag{3.12}$$

Now, in the second step, the evolved state $\Lambda[\rho^{|m_1}]$ is measured and outcome m_2 is obtained whose probability is given by $p(m_2;t_2 \mid m_1) = (1-\lambda)\,\delta_{m_1,m_2} + \lambda\; p(m_2;t_1)$. This $p(\mathbf{m};t_2 \mid m_1)$ will be again a semi-Gaussian distribution with a conditional mean and conditional standard deviation

$$\begin{aligned} \mathbb{E}[\mathbf{m};t_2 \mid m_1] &= (1-\lambda)\,m_1 \\ \sigma[\mathbf{m};t_2 \mid m_1] &= \sqrt{\lambda\,(\frac{N}{4} + (1-\lambda)\,m_1^2)} \end{aligned} \tag{3.13}$$

Thus, the second measurement statistics are correlated with the first measurement outcome m_1. This correlation does not last forever and is limited by the relaxation time of the dissipative system, T. For instance, if we record data so slowly, $\delta t >> T$(or $\lambda \to 1$), each measurement data m_k is sampled from a fixed distribution $p(\mathbf{m};t_1)$ with zero mean and $\frac{1}{2}\sqrt{N}$ standard deviation and there will be no correlation between data, Equation 3.13. In another extreme case, when we record data quickly, $\delta t << T$, then $1-\lambda \approx 1-\frac{\delta t}{T}$ and the system does not evolve, hence, the data is repeatable, which is a property of a projective measurement. In non-extreme regimes, when $\delta t < T$, the data is sampled from semi- binomial distributions whose mean and variance are fluctuating from one measurement to another.

After a long data acquisition a list of outcomes $\{m_1, m_2, ..., m_k\}$ is obtained which constructs the spin noise signal. The spin noise is the net magnetization of an ensemble whose fluctuating

value is bounded by $\frac{N}{2}$ and -$\frac{N}{2}$. At step k^{th}, m_k is a random variable sampled from semi-Gaussian distribution $p(\mathbf{m};t_k \mid m_{k-1},...,m_2,m_1)$ whose mean and variance are correlated with previous recorded data. For the particular choice of a depolarizing map, using inductive reasoning, we obtain that the the joint probability distribution between any two data points is

$$\begin{aligned} p(m_i;t_i,\ m_j;t_j) &= (1-\lambda)^{i-j}\ \delta_{m_i,m_j}\ p(m_j;t_j) \\ &+ \eta_{i-j}\ p(m_i;t_i)\ p(m_j;t_j) \end{aligned} \tag{3.14}$$

where $\eta_k = \lambda + (1-\lambda)\ \eta_{k-1}$ and $\eta_0 = 0$ and $p(m;t_i) = p(m;t_1) = Tr[\Pi_m \rho_0]$. Equation 3.14 indicates that, with the probability of $(1-\lambda)^k \sim e^{-t_k/T}$, the two measurements separated by $t_k = k\ \delta t$, are perfectly correlated and with the probability of η_k, they are two independent random variables. In other words, the closer the two measurements are in time, the more likely that their distributions are correlated. Given Equation 3.14, one can compute the covariance function as a measure of the correlation

$$\begin{aligned} R(k) &\equiv \mathbb{E}[\mathbf{m};t_{k+i}\ ,\ \mathbf{m},t_i] - \mathbb{E}[\mathbf{m};t_{k+i}]\ \mathbb{E}[\mathbf{m},t_i] \\ &= \frac{N}{4}\ e^{-t_k/T} \end{aligned}$$

where the expectation values are calculated using $\mathbb{E}[X;t_1] = \sum_x\ x\ p(x;t_1)$ and $\mathbb{E}[X;t_i\ ,\ Y;t_j] = \sum_{xy}\ x\ y\ p(x;t_i\ ,\ y,t_j)$ and we assumed an initially fully mixed state.

This analysis has considered a collective evolution Λ and a collective measurement Π_m over an ensemble where the collective measurement preserves coherences within the subspace m.

3.3.1 Arbitrary Quantum Map Λ for non-interacting spins

We can further generalize the description by extending it to any arbitrary CPTP quantum map acting on individual spins. More precisely, suppose the spins are not interacting with each other, that there is no field inhomogeneity and also no variation of the B_1 field, and, that each individual spin interacts with its own bath. Therefore, spins are indistinguishable to the environment and one can model the ensemble quantum evolution as $\Lambda = \Phi^{\otimes N}$ where Φ is a CPTP map on a single spin. In this picture, each spin is an open quantum system.

As before, consider a totally mixed initial state for each spin, $\rho_0 = (\frac{\mathbb{1}}{2})^{\otimes N}$, and make a strong measurement along the z axis. Upon the measurement with outcome m, there are $\frac{N}{2}+m$ number of spins with up orientation and $\frac{N}{2}-m$ with down orientation. So, the measurement statistics are

given by

$$p(\mathbf{m};t_1) \;=\; \left(\begin{array}{c} N \\ \frac{N}{2}+m \end{array} \right) (\frac{1}{2})^{\frac{N}{2}+m} (\frac{1}{2})^{\frac{N}{2}-m}. \tag{3.15}$$

The PVM operator given in Eq.(1) can also be expanded in the tensor product basis as:

$$\Pi_m = \sum_p \hat{\mathscr{P}}_p [|\uparrow\rangle\langle\uparrow|^{\otimes \frac{N}{2}+m} \otimes |\downarrow\rangle\langle\downarrow|^{\otimes \frac{N}{2}-m}].$$

Here, since the spins are indistinguishable, there is a sum over all possible spin permutations that results in net spin magnetization m. So, $p \in \{1,...,\left(\begin{array}{c} N \\ \frac{N}{2}+m \end{array} \right)\}$. Upon recording the classical value m_1, the density matrix is updated to

$$\begin{aligned} \rho^{|m_1} &= \frac{\Pi_{m_1}\, \rho_0\, \Pi_{m_1}}{p(m_1;t_1)} \\ &= \frac{\sum_s \hat{\mathscr{P}}_s [|\uparrow\rangle\langle\uparrow|^{\otimes \frac{N}{2}+m_1} \otimes |\downarrow\rangle\langle\downarrow|^{\otimes \frac{N}{2}-m_1}]}{2^N p(m_1;t_1)}. \end{aligned} \tag{3.16}$$

This updated state evolves under Λ which means that each spin evolves under Φ. An example of a single qubit CPTP map Φ would be a rotation around axis $\hat{r}_1$, a relaxation around axis $\hat{r}_2$ and a dephasing around axis $\hat{r}_3$ on the Bloch sphere. In general, the action of a map Φ on the spin basis can be written as

$$\Phi[|\uparrow\rangle\langle\uparrow|] = (1-\alpha)\,|\uparrow\rangle\langle\uparrow| + \alpha\,|\downarrow\rangle\langle\downarrow| + \text{Off diagonal},$$

$$\Phi[|\downarrow\rangle\langle\downarrow|] = (1-\beta)\,|\downarrow\rangle\langle\downarrow| + \beta\,|\uparrow\rangle\langle\uparrow| + \text{Off diagonal},$$

where α and β are variables which are determined by the map's parameters such as evolution time δt, frequency ω, relaxation and dephasing rates and the directions $\hat{r}_1, \hat{r}_2, \hat{r}_3$.

The second measurement on $\Lambda[\rho^{|m_1}]$ results in outcome m_2 which occurs with probability

$$\begin{aligned} p(m_2;t_2 \mid m_1) = \sum_{k=0}^{\frac{N}{2}+m_1} \sum_{l=0}^{\frac{N}{2}-m_1} \quad & \{\text{Bin}(\frac{N}{2}+m_1,k,\alpha) \\ & \text{Bin}(\frac{N}{2}-m_1,l,\beta)\delta_{m_2-m_1,l-k}\}, \end{aligned} \tag{3.17}$$

where $\mathrm{Bin}(n,k,p) = \left(\begin{array}{c} n \\ k \end{array} \right) p^k (1-p)^{n-k}$. This new distribution is again a binomial with mean value

$$\mathbb{E}[\mathbf{m}, t_2 \mid m_1] = m_1(1-(\alpha+\beta)) + (\frac{N}{2})(\alpha-\beta),$$

and standard deviation

$$\begin{aligned} \sigma[\mathbf{m}; t_2 \mid m_1] &= \sqrt{\frac{N}{2}(\alpha(1-\alpha)+\beta(1-\beta)} \\ &+ \sqrt{m_1(\alpha(1-\alpha)-\beta(1-\beta)}. \end{aligned}$$

As the above relations indicate, depending on the evolution map's parameters, α and β, the statistics of the noise are different. Nevertheless, the spin noise magnitude still scales with $\sqrt{N}$ and exhibits a time correlation. Notice, it is not necessary to consider an open system interacting with an environment to see the spin fluctuation. For example, even in the case of simple unitary evolution where $\alpha = \beta = \sin^2[\omega\ \delta t]$, these correlated fluctuations exist.

In order to find the correlation function, we need to know the joint probability distribution, Equation 3.15. In the particular choice of a totally mixed input state, after each measurement, the updated density matrix is $\Pi_{m_k}/Tr[\Pi_{m_k}]$. Therefore, $p(m_k;t_k \mid m_{k-1}) = p(m_2;t_2 \mid m_1)$ for all t_k, and hence, the joint probability distribution of any two data points is:

$$\begin{aligned} p(m_i;t_i\ ,\ m_j;t_j) &= \sum_{l_{i-j},\ldots,l_{i-1}} p(m_i;t_i \mid l_{i-1}) \\ &\quad \times \ldots \times\ p(l_{i-j};t_{i-j} \mid m_j) p(m_j;t_j). \end{aligned} \tag{3.18}$$

Substituting Equation 3.17 into Equation 3.18 gives us an analytic expression for the joint probability distribution and in the large ensemble limit and for the totally mixed input state, one can approximate each $p(m_k,t_k \mid m_{k-1})$ with a Gaussian distribution whose mean and variance are fluctuating from one measurement to the next.

3.3.2 Arbitrary Initial State

In this section, we consider N identical and non interacting spins $\rho_0 = \rho^{\otimes N}$, where ρ is an arbitrary single spin density matrix that is expanded as

$$\rho = a \mid\uparrow\rangle\langle\uparrow\mid + (1-a) \mid\downarrow\rangle\langle\downarrow\mid + b \mid\uparrow\rangle\langle\downarrow\mid + b^* \mid\downarrow\rangle\langle\uparrow\mid. \tag{3.19}$$

The first measurement on this ensemble results in the statistical distribution

$$p(m_1;t_1) \;=\; \left(\begin{array}{c} N \\ \frac{N}{2}+m \end{array} \right) (a)^{\frac{N}{2}+m_1}(1-a)^{\frac{N}{2}-m_1}. \tag{3.20}$$

This distribution does not distinguish ρ from a diagonal state $\tilde{\rho} = a \mid\uparrow\rangle\langle\uparrow\mid + (1-a) \mid\downarrow\rangle\langle\downarrow\mid$ since the measurement is along the z axis. Therefore, it is sufficient to consider $\tilde{\rho}$ as an arbitrary initial state. Upon the strong measurement given by Π_m, the state update rule implies that

$$\begin{aligned} \rho^{|m_1} \;&=\; \sum_s (a)^{\frac{N}{2}+m_1}(1-a)^{\frac{N}{2}-m_1} \\ &\times\; \frac{\hat{\mathscr{P}}_s\left[\mid\uparrow\rangle\langle\uparrow\mid^{\otimes\frac{N}{2}+m_1} \otimes \mid\downarrow\rangle\langle\downarrow\mid^{\otimes\frac{N}{2}-m_1}\right]}{p(m_1;t_1)}. \end{aligned} \tag{3.21}$$

By replacing $p(m_1;t_1)$ with Equation 3.20, we see that the above state is identical to the updated state in Equation 3.16, where the experiment started from a mixed state. Despite the fact that the first measurement statistics differentiate an arbitrary initial state (ρ or $\tilde{\rho}$) from an identity state ($\mathbb{1}/2^N$), their corresponding updated states are no longer distinguishable to the subsequent measurement-evolution processes. As a result, except for the first data point, the statistical fluctuations of spin noise are the same whether we start from a mixed state or from an arbitrary initial state.

3.4 Weak Measurement Model

In an NMR measurement, it is too idealistic to assume that the detection process can resolve a single spin. If we relax this assumption, the projective measurement operators $\mathscr{M}_m = \Pi_m$, no longer describe the action of a measurement. One needs to assign a width of precision to the measurement apparatus which results in an overlap between the different subspaces (Figure 3.2). Therefore, once the data m_0 is recorded, the spin ensemble density matrix collapses not only to the m_0 subspace but also to other subspaces with $l \neq m_0$. As stated before, a PVM is a special case of generalized measurement that is described by positive valued operator measure (POVM) operators, $\{E_m\}$, which result in measurement statistics $p(m) = Tr[E_m\ \rho]$, [20]. Therefore, we adapt the spin noise model by relaxing the assumption of a strong measurement to a weak measurement and defining POVM elements, $E_m = \mathscr{M}_m^\dagger \mathscr{M}_m$, as a sum of PVM operators,

$$E_m = \sum_{l=-N/2}^{N/2} D(m,l)\ \Pi_l \tag{3.22}$$

where $D(m,l)$ is a two variable function whose form is limited by physical constraints:

1. The measurement is trace preserving. So,

$$\sum_m E_m = \mathbb{1} \;\Rightarrow\; \text{for each } l \;\; \sum_m D(m,l) = 1.$$

   This means that D is certainly a distribution relative to m, but it does not have to be a distribution relative to l. This condition becomes particularly important when we get close to the boundaries $\pm\frac{N}{2}$.

2. Since the detector records data m as the outcome, we expect D to have its maximum value at $l = m$. So,

$$\max_l D(m,l) = D(m,m).$$

3. In a weak measurement, the measurement outcome is less reliable; if the measurement apparatus records m, there is a probability $D(m,l)$ that the updated system collapses to other subspaces with $l \neq m$. One expects the further apart l and m are, the less likely it is to collapse into the l subspace. Thus, $D(m,l)$ should decrease as $|l-m|$ increases and its width should be inversely proportioned to the reliability of the measurement device, $1/w$.

4. D need not be a symmetric function. For instance, we know it must be a distribution relative to m but it need not have restriction relative to l. So, in general $D(a,b) \neq D(b,a)$.

Considering the above constraints, we model the function $D(m,l)$ by a semi-Gaussian distribution

$$D(m,l) = A_l \; e^{\frac{-(m-l)^2}{2w^2}} \text{ where } A_l = (1/\sum_k e^{\frac{-(k-l)^2}{2w^2}}). \tag{3.23}$$

In this model, we quantify the "weakness" of the measurement by the quantity w. In the extreme limit of a "strong" measurement, when $w \to 0$, D becomes sharp, i.e., $D(m,l) \to \delta(m-l)$, and hence, $E_m \to \Pi_m$ (Figure 3.2). In the limit of a "very weak" measurement when $w \to \infty$, $D(m,l)$ becomes a uniform distribution and hence $E_m \propto \mathbb{1}$, and so, the state ρ_0 is not affected by the state update rule. In other words, the weakest measurement causes the least disturbance to the system.

Consider an ε-polarizing quantum map, $\Lambda[\rho] = (1-\lambda)\,\rho + \lambda\;\rho_0$, for the evolution process which tends to return the state to the thermal equilibrium polarization with $Tr[\mathbf{S}_z\rho_0] = \varepsilon$. As an example, consider the initial state $\rho_0 = \sum_k q_0(k)\;\frac{\Pi_k}{Tr[\Pi_k]}$ in which $q_0(k)$ is a density function with mean value $\varepsilon = \sum_k k\; q_0(k)$. For instance, in the case of a mixed state, $\rho_0 = \frac{\mathbb{1}}{2^N}$, $q_0(k) = Tr[\Pi_k]/2^N$

is a binomial distribution with zero mean. Given ρ_0, the first weak measurement results in m_1 with a probability

$$\begin{aligned} p(m_1;t_1) &= Tr[E_{m_1}\rho_0] \\ &= \sum_k D(m_1,k)\ q_0(k). \end{aligned} \tag{3.24}$$

It is known that given the distribution $p(m)$, the updated density matrix is not uniquely determined in case of a weak measurement, [20]. This is because, the set of $\{\mathscr{M}_m\}$ that satisfies $\mathscr{M}_m^\dagger \mathscr{M}_m = E_m$ is not unique. Nevertheless, one of the possible ways of updating the density matrix is $\mathscr{M}_m = \sqrt{E_m}$, which gives

$$\begin{aligned} \rho^{|m_1} &= \frac{\sqrt{E_{m_1}}\rho_0.\sqrt{E_{m_1}}}{p(m_1;t_1)}, \\ &= \sum_k \frac{D(m_1,k)\ q_0(k)}{p(m_1)}\ \frac{\Pi_k}{Tr[\Pi_k]}, \\ &= \sum_k q_1(k \mid m_1)\ \frac{\Pi_k}{Tr[\Pi_k]}. \end{aligned}$$

Here, we define $q_1(k \mid m_1) := \frac{D(m_1,k)\ q_0(k)}{p(m_1;t_1)}$ to be the updated density function. As desired, the updated density matrix collapses not only to $\frac{\Pi_m}{Tr[\Pi_m]}$ but also to other neighbouring subspaces, $k \neq m_1$, and its range depends on the measurement "weakness" w. This semi-localized state around m_1, will then evolve under the ε-polarizing map, Λ. Similar to the PVM case, by performing the second measurement, we obtain a conditional distribution

$$\begin{aligned} p(m_2;t_2 \mid m_1) &= Tr[E_{m_2}\ \Lambda[\rho^{|m_1}]] \\ &= (1-\lambda)\ \sum_k D(m_2,k)\ q_1\ (k \mid m_1) \\ &+ \lambda\ \sum_k D(m_2,k)\ q_0(k). \end{aligned}$$

The fact, the overlap between $D(m_2,l)$ and $D(m_1,l)$ that appears in the first term of the last equation, confirms that as long as $\lambda \neq 1$ and $w \neq \infty$, there are correlations carrying on from one measurement to another.

We calculated the joint probability distribution between any two data points and obtained

$$\begin{aligned} p(m_i;t_i,m_j;t_j) &= (1-\lambda)^{i-j}\ \sum_l D(m_i,l)\ D(m_j,l)\ q_0(l) \\ &+ \eta_{i-j}\ p(m_i;t_i)\ \ p(m_j;t_j). \end{aligned}$$

Despite the fact that a strong and a weak measurement result in different statistical distributions, (i.e. $Tr[\Pi_m \rho] \neq Tr[E_m \rho]$) there are common features in both limits, most importantly, the statistics of instances are correlated with previous data. These correlations are a result of the quantum evolution map between measurements.

Thus far, we have not included the suggested Gaussian model for $D(m,l)$. If we do so, the covariance function becomes

$$R(k) = \frac{N}{4}\,(1-\lambda)^k + (\eta_k - 1)\;\mathbb{E}[\mathbf{m};t_1)^2]. \tag{3.25}$$

One can test this relation for a totally mixed input state and reproduce the exact result in Equation 3.15. This indicates that spin fluctuations have a similar behaviour in both the strong and the weak measurement limit.

3.5 Example

In this section, we give a concrete example of a spin noise model. Consider 100 spin half particles each oriented randomly in the Bloch sphere, $\rho_0 = (\frac{\mathbb{1}}{2})^{\otimes N}$. At $t = t_1$, we measure the magnetization along the z axis, so, the single shot measurement outcome m, is the z component of the ensemble's magnetization, i.e. $m = \sum_{i=1}^{100} s_i$ with $s_i = \pm\frac{1}{2}$. Thus, $m \in \{-50,-49,...,0,...,49,50\}$ is a random number sampled from the probability distribution $p(\mathbf{m};t_1)$. Given the totally mixed initial state

$$\begin{aligned} p_{st}(\mathbf{m};t_1) &= Tr[\Pi_{\mathbf{m}}\;\rho_0] = \mathrm{Bin}(N, \frac{N}{2}+\mathbf{m}, \frac{1}{2}), \\ p_{wk}(\mathbf{m};t_1) &= Tr[E_{\mathbf{m}}\;\rho_0] = \sum_{k=-\frac{N}{2}}^{\frac{N}{2}} D(\mathbf{m},k)\;\mathrm{Bin}(N, \frac{N}{2}+k, \frac{1}{2}), \end{aligned} \tag{3.26}$$

where the subscript *st* (or *wk*) refers to the strong (or the weak) measurement. If one repeats this first measurement with the same initial state, ρ_0, many times, a statistical distribution of $\mathbf{m}(t_1)$ will be obtained. We implemented this numerically and the results are shown in Figure 3.5. Once the data m_1 is recorded, the ensemble's density matrix is updated to

$$\rho^{|m_1} = \frac{\Pi_{m1}}{2^N p_{st}(m_1;t_1)}, \qquad \text{or} \qquad \rho^{|m_1} = \frac{E_{m1}}{2^N p_{wk}(m_1;t_1)} \tag{3.27}$$

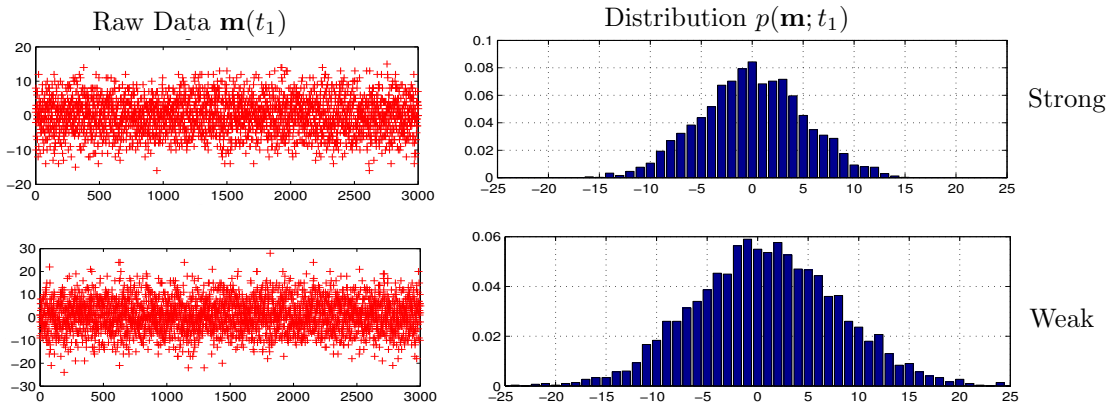

Figure 3.5: 3000 identical measurements are performed on 3000 identically prepared spin states with $\rho_0 = (\frac{\mathbb{1}}{2})^{\otimes N}$. Each data point is a random number m_1 sampled from the statistical distribution $p(\mathbf{m};t_1)$. A numerical estimation of $p(\mathbf{m};t_1)$ is computed and plotted on the right side for both strong and weak measurements. $N = 100$ and $w = 5$.

depending on whether the measurement was strong or a weak. Now, we let the spin system evolves for certain time δt under the following quantum evolution map

$$\begin{aligned} \Lambda[\rho] &= \Phi^{\otimes N}[\rho] \quad \text{where} \\ \Phi[\rho] &= (1-\lambda)\, U_x\, \rho\, U_x^\dagger + \lambda \frac{\mathbb{1}}{2}. \end{aligned} \tag{3.28}$$

The CPTP map Φ acts on individual spins, and for this example, we chose it to be a depolarizing map (relaxation) followed by a unitary rotation around the x axis, i.e., $U_x = e^{-i\omega S_x \delta t}$. Φ is parametrized by $\lambda = 1 - e^{-\delta t/T}$ and $\theta = \omega\ \delta t$. Following the discussion in Section 3.3.1, the probability of spin flip is $\alpha = \beta = (1-\lambda)(\sin\theta)^2 + \frac{\lambda}{2}$. Following the spin noise model, once the system is measured and evolves under Λ, the second measurement is performed at $t = t_2$. The second measured outcome $m_2 \in \{-50, -49, ..., 0, ..., 49, 50\}$ is again a random number sampled from the conditional probability distribution $p(\mathbf{m};t_2 \mid m_1)$. For this particular example and in

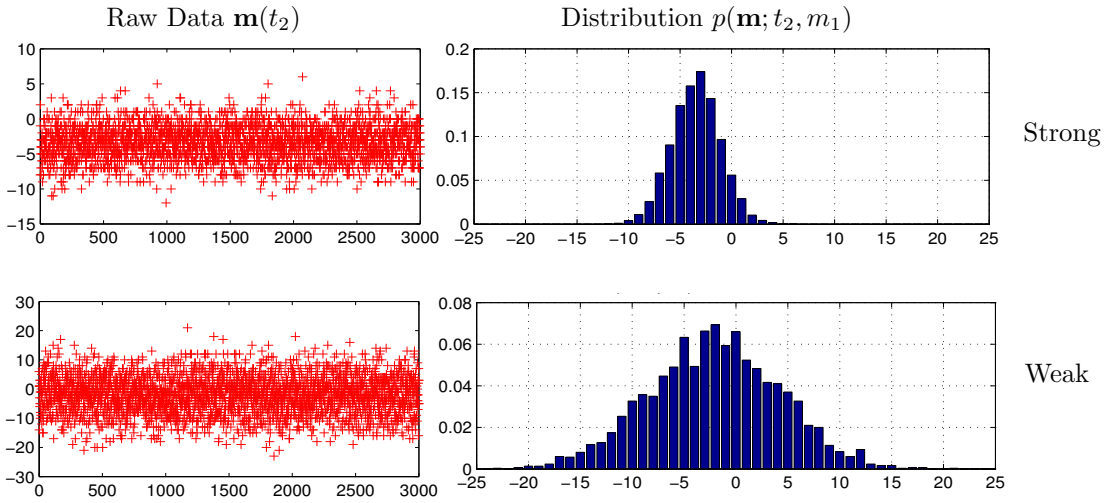

Figure 3.6: The raw data (left) and its corresponding statistical distribution (right) of the second measurement is presented for both cases of the strong and the weak measurements. Here, $\lambda = 0.1$ and a small unitary rotation, $\theta = \pi/32$, are considered.

case of the strong measurement, we obtain

$$\begin{aligned} p_{st}(\mathbf{m};t_2 \mid m_1) &= Tr[\Pi_{\mathbf{m}}\, \Lambda[\rho^{|m_1}]] \\ &= \sum_{i=0}^{\frac{N}{2}+m_1} \mathrm{Bin}(\frac{N}{2}+m_1,i,\alpha) \\ &\times \mathrm{Bin}(\frac{N}{2}-m_1,\mathbf{m}-m_1+i,\alpha) \end{aligned} \tag{3.29}$$

and in case of the weak measurement

$$\begin{aligned} p_{wk}(\mathbf{m};t_2 \mid m_1) &= Tr[E_{\mathbf{m}}\, \Lambda[\rho^{|m_1}]] \\ &= \sum_{k,k'=-\frac{N}{2}}^{\frac{N}{2}} D(\mathbf{m},k)\, D(m_1,k')\, \mathrm{Bin}(N,\frac{N}{2}+k',1/2) \\ &\times \frac{p_{st}(k;t_2 \mid k')}{p_{wk}(m_1;t_1)} \end{aligned} \tag{3.30}$$

For the numerical simulation, we prepared identical initial states ρ_0, performed the first measurement on them, then post selected on that data with magnetization value $\mathbf{m} = m_1$. Given, these

selected conditional states $\Lambda[\rho^{|m_1}]$, we made a second measurement and recorded the data and its statistics as shown in Figure 3.6.

To see the correlation between the two subsequent data points, we plot the joint probability distribution $p(\mathbf{m}_2, \mathbf{m}_1) = p(\mathbf{m}_2 \mid \mathbf{m}_1)p(\mathbf{m}_1)$ where $\mathbf{m}_i = \mathbf{m}(t_i)$. As shown in Figure 3.7, for the case of $\lambda = 0$, $\theta = 0$ (no evolution) and strong measurement, there is a maximum correlation between the two data points. But, for the case of weak measurement, there is less correlation even in the absence of any evolution. This shows that the data may not be reproducible in the case of a weak measurement. As the spin flip probability, α, becomes larger (longer evolution), the two data points become less and less correlated as seen in Figure 3.7.

3.6 Summary

An open quantum system model of the spin noise signal in NMR was described. We have shown that the inherent spin fluctuations can be described by the nature of quantum measurements, the state update rule and quantum evolution. We analysed our model for arbitrary initial states including the identity, as well as any arbitrary quantum evolution CPTP map acting on non-interacting spins, with the depolarizing map as an example of a collective quantum evolution. We calculated the joint probability distribution and the covariance function for different examples in both the limits of strong and weak measurement.

The proposed spin noise model predicts the statistical fluctuation of a spin ensemble by considering a collective measurement and a collective quantum evolution while retaining the average properties such as thermal polarization. Previous computational models of spin noise have introduced a fluctuating field over the ensemble to create dephasing and account for noise correlations, [52].

Here, the model does not require such a field, the fluctuations are a function of the update rule that propagates over knowledge of the system. This analysis is intended to illustrate that with a description of the spin, the cavity and the bath interactions one may straightforwardly calculate the properties of spin noise, including its correlation function. Such descriptions are useful in analysing experimental instances of spin noise, in particular, with the development of spin based quantum information processors that have long lived spin states and small number of spins.

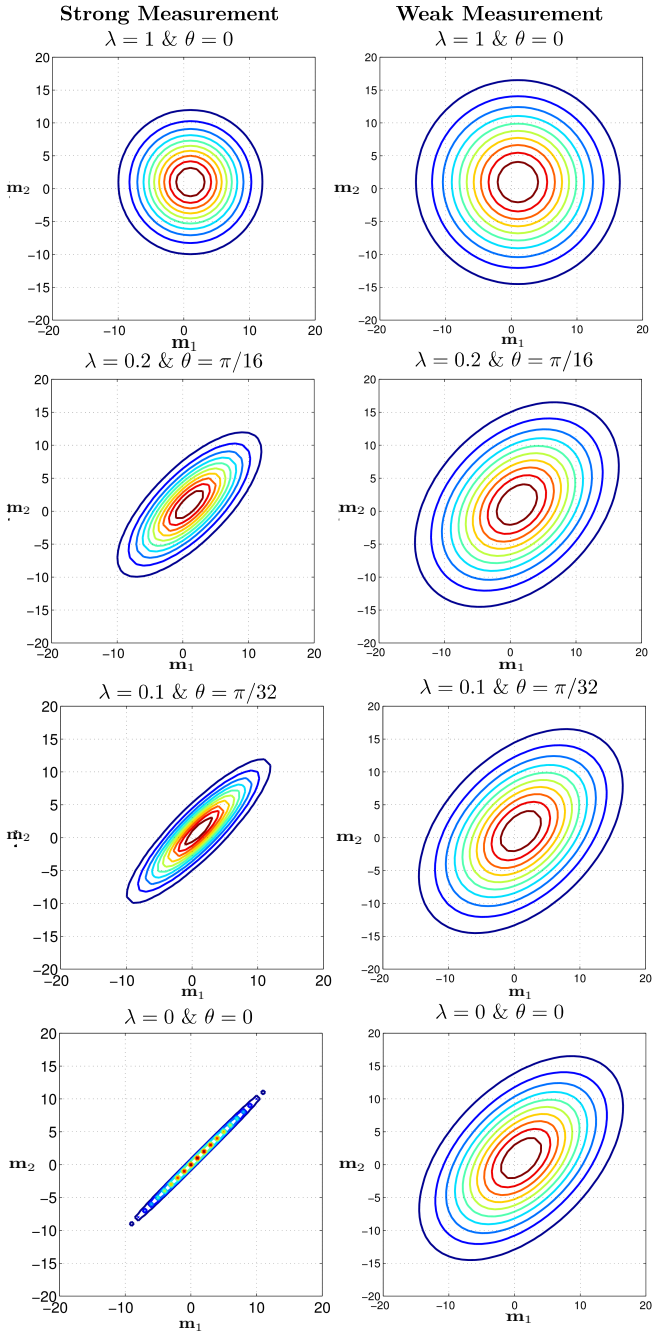

Figure 3.7: Contour plots of the joint probability distribution, $p(\mathbf{m}_2, \mathbf{m}_1)$ for different values of λ and θ. The top figure $\lambda = 1$ and $\theta = 0$, shows no correlation between subsequent data points and the bottom figure $\lambda = 0$ and $\theta = 0$ shows a maximum correlation between them.

Chapter 4

Protection Against Collective Noise In NMR

4.1 Introduction

A two-level system that is a candidate for quantum information processing is called a qubit. If we encode information in the actual physical states, there is always a threat of undesired coupling to the environment, which makes the qubit fragile against noise. For example, a spin half particle may experience a bit flip error (X-noise) that converts $|\uparrow\rangle$ to $|\downarrow\rangle$ or a phase flip error (Z-noise) that corrupts coherence information in a superposition state, $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$. In NMR language these errors may appear as relaxation and decoherence processes.

In quantum information theory, a well-known and common way of protecting information is to use *Quantum Error Correction* techniques, [20, 55]. Regardless of the complexity of QEC algorithms, there is a basic principle that is easy to understand. Typically, information is *encoded* into a logical qubit by adding some ancillary physical qubits and applying certain gates to create a correlation between the logical qubit and the ancillary qubits. In this way, if a particular noise affects information stored in the logical qubit, it leaves a syndrome on the ancillary qubits, and hence, the error is tractable. At the end of a QEC algorithm, the information is *decoded* by *reading* the syndrome and then applying certain gates to the logical qubit to *undo* the effect of noise and recover the information. One issue with various QEC proposals is that the encoding and decoding gates are also subject to errors. In practice, implementation of these error correcting gates requires a high fidelity control. In addition, in order to be useful for quantum computing purposes, these gates mus be fast enough when compared with the physical limiting times, such as T_1 and T_2.

An alternative approach to protecting the information is to encode it in such a way that the logical qubit is not affected by noise in the first place, and so, no error correcting code is required. For example, instead of considering a two-level physical system, one can consider a collection of physical qubits and encode the logical qubit in a collective degree of freedom of this group of qubits such that it is robust against the collective noise. Thus, in this section, we explore the possibility of storing information in a collective degree of freedom of a methyl group, which is a physical candidate for implementing this idea with three identical spins.

In Section 4.2.1, we introduce a collective noise interaction model followed by two well-known methods of encoding a logical qubit into a noise protected space of a group of physical qubits. Next, from Section 4.4 to Section 4.9, we particularly study the electronic, vibration, internal rotation and spin degrees of freedom of a methyl group and their corresponding symmetries. Then, in Section 4.10, we explore the possibility of initializing the collective spin state of the protons in a methyl group into a noise protected state. Finally, in Section 4.11, we analyze the symmetry properties of the dipolar interaction, and discuss how the dipolar relaxation leads to NMR observation of noise protected states.

4.2 Protection Against Collective Noise

4.2.1 Collective Noise Model

Consider N identical spins that are symmetrically coupled to the environment (or the bath). The bath is considered as the noise source, and since it does not distinguish spins, the operators acting on the spin system are simply the total spin angular momentum, i.e., $\hat{\mathbf{S}}_\alpha = \frac{1}{2}\sum_{i=1}^{N}\sigma_\alpha^{(i)}$, where $\alpha = x,y,z$ and $\hbar = 1$. The total Hamiltonian of this composite closed system is

$$H_{sb} = H_s + H_b + \sum_\alpha \hat{\mathbf{S}}_\alpha \otimes \hat{B}_\alpha, \tag{4.1}$$

where the first two terms are individual spin and bath Hamiltonians, and the last term is the interaction between them. Given the above Hamiltonian, the time evolution of the spin-bath system is given by $U_{sb} = e^{-iH_{sb}t}$.

Definition 4.1. The interaction algebra, $\mathbb{J}$, is a linear span of all sums and products of the system interaction operators, $\{\hat{\mathbf{S}}_\alpha\}$, with an inclusion of the identity operator, i.e., $\mathbb{J} = \{\mathbb{1}, \hat{\mathbf{S}}_x, \hat{\mathbf{S}}_y, \hat{\mathbf{S}}_z, \dots\}$.

Suppose that the system and the bath are initially uncorrelated, $\rho_0 = \rho_s \otimes \rho_b$. According to the system-environment representation in Equation 2.47, the reduced dynamic of the spin system

is represented by $\mathscr{E}[\rho_s] := Tr_b[U_{sb}\ \rho_s \otimes \rho_b\ U_{sb}^\dagger]$. As discussed before, $\mathscr{E}[.]$ is a CPTP map that represents the *collective quantum noise channel*. In the above noise model, the group of identical spins is considered as an open quantum system experiencing a collective noise, $\mathscr{E}[.]$, with the Kraus representation

$$\mathscr{E}[\rho_s] = \sum_\alpha K_\alpha\ \rho_s\ K_\alpha^\dagger. \tag{4.2}$$

Here, $K_\alpha \in \mathbb{J}$ are the elements of the interaction algebra, and hence named *noise operators*.

We wish to initialize the spin system in a *protected* quantum state such that it is robust against the above collective noise model. In the following, we first briefly introduce the notions of decoherence free subspaces and noiseless subsystems, as two well-known examples of protected states. For a review on these notions, we refer to [56–58]. Further, for the rest of this chapter, we explore the possibility of experimentally creating a protected state in a methyl group.

4.2.2 Decoherence Free Subspace

Suppose we could decompose the Hilbert space into two parts: one that is *protected* against noise and is labelled with p and the other that is affected by *noise* and is labelled with n. Intuitively, if we encode information in just the *noise free* subspace, the information is not corrupted by noise, and so, QEC is not required. Mathematically, suppose we could write the Hilbert space as a direct sum of two subspaces, i.e., $\mathscr{H} = \mathscr{H}_p \oplus \mathscr{H}_n$. In the same manner, we decompose the density matrix to $\rho = \rho_p \oplus \rho_n$, where $\rho_p \in \mathbf{L}(\mathscr{H}_p)$ and $\rho_n \in \mathbf{L}(\mathscr{H}_n)$. Suppose that the noise operator can also be repartitioned as $K_\alpha = U \oplus \mathscr{N}_\alpha$ in which U is a unitary operator and $\{\mathscr{N}_\alpha\}$ is a set of Kraus operator that satisfy $\sum_\alpha \mathscr{N}_\alpha^\dagger \mathscr{N}_\alpha = \mathbb{1}$. Then, Equation 4.2 becomes

$$\begin{aligned} \mathscr{E}[\rho] &= \sum_\alpha (U \oplus \mathscr{N}_\alpha)\ (\rho_p \oplus \rho_n)\ \left(U^\dagger \oplus \mathscr{N}_\alpha^\dagger\right) \\ &= U\ \rho_p\ U^\dagger \oplus \sum_\alpha \mathscr{N}_\alpha\ \rho_n\ \mathscr{N}_\alpha^\dagger. \end{aligned} \tag{4.3}$$

If the information of interest is initially stored in the $\rho_p \in \Gamma(\mathscr{H}_p)$, under the above quantum noise model, the information *remains* in that subspace and is not *lost*. Therefore, the subspace $\mathscr{H}_p$ is *protected* against noise, whereas the subspace $\mathscr{H}_n$ is *noisy*. This is known as Decoherence Free Subspace (DFS).

We clarify the concept of DFS by elaborating on a simple example of two identical nuclear spins. One may expand an arbitrary initial state of two spins in the computational basis,

$$\mathfrak{B}_c(\mathscr{H}_{1/2}^{\otimes 2}) = \{|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle\}, \tag{4.4}$$

or in the total spin angular momentum basis, $\mathfrak{B}_{an}(\mathscr{H}_{1/2}^{\otimes 2}) = \mathsf{Span}\{|j,m_j\rangle\}$, where $\{j\}$ are eigenvalues of $\vec{\mathbf{S}}$ and $\{m_j\}$ are eigenvalues of $\mathbf{S}_z$. The spin addition rules imply $j = \frac{1}{2} \otimes \frac{1}{2} = 1 \oplus 0$ and $m_j \in \{0, \pm 1\}$. It is common to name the $j = 1$ states as the *Triplet states*, which are denoted by $|T,m\rangle$ with $m \in \{+1,0,-1\}$. In addition, the $j = 0$ state is known as the *singlet state*, which is denoted by $|S,m\rangle$ with $m = 0$. Correspondingly, the Hilbert space is decomposed to $\mathscr{H} = \mathscr{H}_T \oplus \mathscr{H}_S$, where $\dim(\mathscr{H}_T) = 3$ and $\dim(\mathscr{H}_S) = 1$. The explicit form of these eigenstates are given in Table 4.1.

$\lvert j,m_j\rangle$	Expansion in $\mathfrak{B}_c(\mathscr{H}_{1/2}^{\otimes 2})$
$\lvert T,+1\rangle$	$\lvert\uparrow\uparrow\rangle$
$\lvert T,\ 0\rangle$	$\frac{1}{\sqrt{2}}(\lvert\uparrow\downarrow\rangle + \lvert\downarrow\uparrow\rangle)$
$\lvert T,-1\rangle$	$\lvert\downarrow\downarrow\rangle$
$\lvert S,\ 0\rangle$	$\frac{1}{\sqrt{2}}(\lvert\uparrow\downarrow\rangle - \lvert\downarrow\uparrow\rangle)\rangle$

Table 4.1: The expansion of the angular momentum basis in terms of the computational basis for two spins.

In this simple example, the one dimensional subspace $\mathscr{H}_S$ is protected against all collective noise, because, $|S,0\rangle$ has no spin angular momentum. To see this from another angle, we expand the singlet state in the Pauli operator basis,

$$|S,0\rangle\langle S,0| = \frac{1}{2}\left(\mathbb{1} - \vec{\sigma}^{(1)}.\vec{\sigma}^{(2)}\right). \tag{4.5}$$

The appearance of the scalar term $\vec{\sigma}^{(1)}.\vec{\sigma}^{(2)}$, ensures that the singlet state is invariant under all components of the total spin angular momentum, $\hat{\mathbf{S}}_\alpha = \frac{1}{2}\ (\sigma_\alpha^{(1)} + \sigma_\alpha^{(2)})$ with $\alpha \in \{x,y,z\}$. Therefore, the $j = 0$ subspace of two identical spins is a DFS.

Note that this one dimensional subspace is not enough to define a qubit for quantum computation, nevertheless, it might be useful for other purposes. For example in NMR, one of the common sources of T_2 relaxation or the dephasing is the noise along the z axis. On the other hand, we know $\{|T,0\rangle, |S,0\rangle\}$ are both eigenstates of $\hat{\mathbf{S}}_z$, thus, they are protected against collective dephasing noise. Therefore, it seems reasonable to initialize the two spin system in $\rho = \frac{1+\varepsilon}{2}\ |S,0\rangle\langle S,0| + \frac{1-\varepsilon}{2}\ |T,0\rangle\langle T,0|$, since a part of this state is protected against all collective noise and the rest is protected against collective dephasing noise. As a result, it is expected that $|\psi\rangle$ exibits long relaxation times. This has been experimentally demonstrated in [59–61], where some imbalance of population is created between $|S,0\rangle\langle S,0|$ and $|T,0\rangle\langle T,0|$, and the state is referred to as a *Long Lived State* (LLS).

One can extend this idea to $N=4$ physical qubits and look for a DFS. In that case, the singlet subspace, $j=0$, has degeneracy of 2. As such, the degeneracy degree of freedom is a good candidate for defining a logical basis. Explicitly,

$$\begin{aligned} |\bar{0}\rangle &\equiv |j=0,\ m_j=0,\ d=1\rangle \\ &= |S,0\rangle_{12}\otimes|S,0\rangle_{3,4}, \\ |\bar{1}\rangle &\equiv |j=0,\ m_j=0,\ d=2\rangle \\ &= \frac{1}{\sqrt{3}}\left(|T,+1\rangle_{12}\otimes|T,-1\rangle_{3,4}+|T,-1\rangle_{12}\otimes|T,+1\rangle_{3,4}-|T,0\rangle_{12}\otimes|T,0\rangle_{3,4}\right). \end{aligned} \tag{4.6}$$

Here, the indexes $1,2,3,4$ refers to the spin number. For higher number of spins, $N>4$, the number of degenerate states in the subspace of $j=0$ increases, and hence, the $j=0$ subspace might be useful for implementing a qutrit (quantum 3-level system) or a qdit (quantum d-level system). For $N=3$, which is the case under study, such a DFS cannot be defined. We refer to [56] for further information.

4.2.3 Noiseless Subsystem

The idea of decoherence free subspace (DFS) can be extended to *noiseless subsystems* (NS) where a *factor* of a subspace is protected rather than the whole subspace, [62–64]. The basic idea is that a subspace might be decomposed to a tensor product of two subsystems $\mathscr{H}=\mathscr{H}_p\otimes\mathscr{H}_n$, where the noise operators act trivially (such as identity) on the *noise-free* subsystem, $\mathscr{H}_p$, and act non-trivially on the *noisy* subsystem, $\mathscr{H}_n$. We express this concretely in the following theorem.

Theorem: *For a given interaction model, if the interaction algebra, $\mathbb{J}$, is dagger closed (i.e., x & $x^\dagger\in\mathbb{J}$), the Hilbert space can be decomposed to*

$$\mathscr{H}=\bigoplus_j \mathbb{C}_{p_j}\otimes\mathbb{C}_{n_j}, \tag{4.7}$$

such that every noise operator $K_\alpha\in\mathbb{J}$ is approximated as

$$K_\alpha\cong\bigoplus_j \mathbb{1}_{p_j}\otimes\mathscr{N}_{n_j}. \tag{4.8}$$

Here, the index j refers to the jth irreducible representation, p_j is the dimension of each noiseless subsystem, and n_j is the dimension of each noisy subsystem [56, 64].

We clarify the notion of the noiseless subsystem by providing a concrete example of three indistinguishable spins, which is the emphasis of this chapter. One may expand an arbitrary state

of three identical spins in the computational basis,

$$\mathfrak{B}_c(\mathscr{H}_{1/2}^{\otimes 3}) = \{|\uparrow\uparrow\uparrow\rangle, |\uparrow\uparrow\downarrow\rangle, |\uparrow\downarrow\uparrow\rangle, |\uparrow\downarrow\downarrow\rangle|\downarrow\uparrow\uparrow\rangle, |\downarrow\uparrow\downarrow\rangle, |\downarrow\downarrow\uparrow\rangle, |\downarrow\downarrow\downarrow\rangle\}, \tag{4.9}$$

or in the total spin angular momentum basis denoted by $\mathfrak{B}_{an}(\mathscr{H}_{1/2}^{\otimes 3}) = \text{Span}\{|j, m_j, d_j\rangle\}$, where $\{j\}$ (or $\{m_j\}$) are the eigenvalues of the total spin angular momentum (or its z component) in case of three spins, and the label d_j refers to the d^{th} degenerate state of the j^{th} subspace. Spin addition rules imply $j = \frac{1}{2} \otimes \frac{1}{2} \otimes \frac{1}{2} = \frac{3}{2} \oplus \frac{1}{2} \oplus \frac{1}{2}$, $m_j \in \{\frac{\pm 3}{2}, \frac{\pm 1}{2}\}$ and $d_{3/2} = 1$ and $d_{1/2} \in \{1, 2\}$. We expand $|j, m, d_j\rangle$ in terms of the computational basis in Table 4.2.

$\lvert j, m_j, d_j\rangle$	Expansion in $\mathfrak{B}_c(\mathscr{H}_{1/2}^{\otimes 3})$
$\lvert\frac{3}{2}, \frac{3}{2}, 1\rangle$	$\lvert\uparrow\uparrow\uparrow\rangle$
$\lvert\frac{3}{2}, \frac{1}{2}, 1\rangle$	$\frac{1}{\sqrt{3}}(\lvert\uparrow\uparrow\downarrow\rangle + \lvert\downarrow\uparrow\uparrow\rangle + \lvert\uparrow\downarrow\uparrow\rangle)$
$\lvert\frac{3}{2}, -\frac{1}{2}, 1\rangle$	$\frac{1}{\sqrt{3}}(\lvert\downarrow\downarrow\uparrow\rangle + \lvert\uparrow\downarrow\downarrow\rangle + \lvert\downarrow\uparrow\downarrow\rangle)$
$\lvert\frac{3}{2}, -\frac{3}{2}, 1\rangle$	$\lvert\downarrow\downarrow\downarrow\rangle$
$\lvert\frac{1}{2}, \frac{1}{2}, 1\rangle$	$\frac{1}{\sqrt{2}}(\lvert\uparrow\downarrow\rangle - \lvert\downarrow\uparrow\rangle)\lvert\uparrow\rangle$
$\lvert\frac{1}{2}, -\frac{1}{2}, 1\rangle$	$\frac{1}{\sqrt{2}}(\lvert\uparrow\downarrow\rangle - \lvert\downarrow\uparrow\rangle)\lvert\downarrow\rangle$
$\lvert\frac{1}{2}, \frac{1}{2}, 2\rangle$	$\sqrt{\frac{2}{3}}\lvert\uparrow\uparrow\downarrow\rangle - \sqrt{\frac{1}{6}}(\lvert\uparrow\downarrow\uparrow\rangle + \lvert\downarrow\uparrow\uparrow\rangle)$
$\lvert\frac{1}{2}, -\frac{1}{2}, 2\rangle$	$\sqrt{\frac{2}{3}}(\lvert\downarrow\downarrow\uparrow\rangle) - \sqrt{\frac{1}{6}}(\lvert\uparrow\downarrow\downarrow\rangle + \lvert\downarrow\uparrow\downarrow\rangle)$

Table 4.2: The expansion of the angular momentum basis in terms of the computational basis for three spins.

Correspondingly, the Hilbert space of these 3 spins is decomposed to $\mathscr{H} = \bigoplus_j \mathscr{H}_j = \mathscr{H}_{3/2} \oplus \mathscr{H}_{1/2}$, where $\dim(\mathscr{H}_{3/2}) = 4$ and $\dim(\mathscr{H}_{1/2}) = 4$. Each $\mathscr{H}_j$ is further decomposed into a product of two *subsystems*, where the first component refers to the d_j label and the second component refers to the m_j label,

$$\mathscr{H} = \bigoplus_j \mathbb{C}_{\mathbf{d}_j} \otimes \mathbb{C}_{\mathbf{m}_j} = \mathbb{C}_1 \otimes \mathbb{C}_4 \oplus \mathbb{C}_2 \otimes \mathbb{C}_2. \tag{4.10}$$

We used the bold notation to distinguish the dimension of a label space from its value, i.e., $\mathbf{d}_j = \dim(\{d_j\})$ and $\mathbf{m}_j = \dim(\{m_j\})$.

The degeneracy of each subspace j can be visualized as a *path degree* of freedom in the Bratteli diagram, which is shown in Figure 4.1. There are two ways of getting to $j = 1/2$ point:

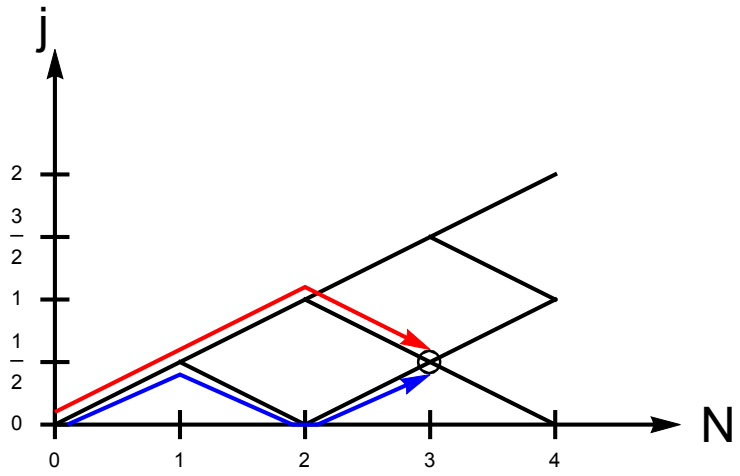

Figure 4.1: Bratteli diagram: The vertical axis is the total spin angular momentum and the horizontal axis is the number of spin half particles.

One way from $0 \oplus \frac{1}{2}$ path and the other way from $1 \oplus \frac{1}{2}$ path. This degeneracy degree of freedom has been used for storing quantum information [63].

In the following, we show that the first component of each subspace, $\mathbb{C}_{\mathbf{d}_j}$, is *preserved* by $\hat{\mathbf{S}}_\alpha$, and only the second component, $\mathbb{C}_{\mathbf{m}_j}$, is affected. We expand $\hat{\mathbf{S}}_z$ in the spin angular momentum basis and obtain,

$$\begin{aligned} \hat{\mathbf{S}}_z &= \sum_{j,m_j,d_j} m \, |j,m_j,d_j\rangle\langle j,m_j,d_j| \\ &= \left(\mathbb{1}_1 \otimes \sum_{m=-3/2}^{+3/2} m \, |m\rangle\langle m| \right) \oplus \left(\mathbb{1}_2 \otimes \frac{\sigma_z}{2} \right). \end{aligned} \tag{4.11}$$

Similarly for $\hat{\mathbf{S}}_x$ we obtain,

$$\hat{\mathbf{S}}_x = \left(\mathbb{1}_1 \otimes \sum_{m=-3/2}^{+3/2} C_m^+ \, |m+1\rangle\langle m| + C_m^- \, |m-1\rangle\langle m| \right) \oplus \left(\mathbb{1}_2 \otimes \frac{\sigma_x}{2} \right), \tag{4.12}$$

where $C_m^\pm = \sqrt{15/4 - m(m\pm 1)}$. As expected, each components of the total spin angular momentum acts trivially (an identity operator or a scalar) on $\mathbb{C}_{\mathbf{d}_j}$. Therefore, we choose the $\mathbb{C}_{\mathbf{d}_j}$ subsystem of the $j = 1/2$ subspace of 3 identical physical qubits to encode one logical qubit

because it is *protected* against collective noise. Explicitly, the logical basis is

$$\begin{aligned} |\bar{0}\rangle &\equiv |j=1/2,\, d_j=1\rangle \otimes |\phi_1\rangle, \\ |\bar{1}\rangle &\equiv |j=1/2,\, d_j=2\rangle \otimes |\phi_2\rangle, \end{aligned} \tag{4.13}$$

where $|\phi_{1(2)}\rangle$ is an arbitrary pure state expanded in the $\mathbb{C}_{\mathbf{m}_{1/2}} = \text{Span}\{|\pm 1/2\rangle\}$ subsystem. Given an arbitrary pure state $|\psi\rangle = a|\bar{0}\rangle + b|\bar{1}\rangle$ with $\sqrt{|\alpha|^2+|\beta|^2} = 1$, the logical qubit is obtained by a partial trace over the $\mathbb{C}_{\mathbf{m}_{1/2}}$ subsystem as

$$\rho_{\text{logic}} = Tr_m[|\psi\rangle\langle\psi|] = \begin{pmatrix} |a|^2 & a^* b\langle\phi_1|\phi_2\rangle \\ b^* a\langle\phi_2|\phi_1\rangle & |b|^2 \end{pmatrix}. \tag{4.14}$$

Note that the off-diagonal terms are proportional to the overlap of $|\phi_1\rangle$ and $|\phi_2\rangle$. This implies that if we prepare $|\phi_1\rangle = |\phi_2\rangle$ perfectly, ρ_{logic} implements an ideal logical qubit, otherwise, any imperfection in the preparation acts as a decoherence process. Note that this type of decoherence is purely due to the imperfections in the state preparation step, not external noise, because all $\hat{\mathbf{S}}_\alpha$ with $\alpha \in \{x,y,z\}$ preserve the overlap $\langle\phi_2|\phi_1\rangle$.

In summary, a noiseless logical qubit can be encoded into the $j = 1/2$ subspace of the collective state of three identical spins. One of the possible candidates for implementing this protected state is the methyl group in a symmetric top molecule, which is the subject of study for the rest of this chapter. In this regard, we study the Hamiltonian and its eigenstructure of a methyl group from the symmetry perspective. This symmetry analysis gives us a great insight about the molecular dynamics which enable us to propose an experiment for encoding a protected state into the collective spin degree of freedom of a methyl group. We also analyze the dipolar relaxation process from the symmetry perspective and discuss how it plays a role in the observation of the protected state. Since the symmetry is the core element of all other sections, in the following, we briefly review some basics from group theory with an emphasis on the C_3 group.

4.3 Symmetry of $\mathbf{C}_3$ Group

$\mathbf{C}_3$ is a group with abstract group elements $\{I, C_+, C_-\}$ and has the following multiplication table,

$\mathbf{C}_3$ is isomorphic to a cyclic permutation group whose elements are the identity operator and

$\mathbf{C}_3$	I	C_+	C_-
I	I	C_+	C_-
C_+	C_+	C_-	I
C_-	C_-	I	C_+

the cyclic permutation of 3 objects which act as

$$\begin{aligned} I\{x,y,z\} &\rightarrow \{x,y,z\}, \\ p_+\{x,y,z\} &\rightarrow \{z,x,y\}, \\ p_-\{x,y,z\} &\rightarrow \{y,z,x\}. \end{aligned} \tag{4.15}$$

One can represent each abstract group element $g \in G$ by a matrix $M(g)$ that acts on a vector space. For example, a rotational transformation in the coordinate system, which consists of a no-rotation matrix ($M(I) = \mathbb{1}$) and ± 120 degree rotational matrices ($M(C_\pm) = R_\pm$), is an isomorphic matrix representation of $\mathbf{C}_3$.

In general, $M(g)$ is not unique, and one may find variety of matrix representations of g that are related to each other by a transformation T, i.e., $M'(g) = T\ M(g)\ T^{-1}$. But, there is one thing common between all matrix representations of g, which is the trace of $M(g)$, because it is invariant under all basis transformations. Therefore, $Tr[M(g)]$ is known as the *character* of g [65]. But, the trace alone is not enough to uniquely describe the matrix representation of a group. Some of the group representations are decomposable, which means that there exist a transformation T to decompose a matrix representation $M(g)$ into a direct sum of other matrix representations with lower dimensions, i.e., $T\ M(g)\ T^{-1} = M^{(1)}(g) \oplus M^{(2)}(g) \oplus \cdots \oplus M^{(k)}(g)$. If the *same* transformation is applied to all elements of a specific matrix representation and they are *all* decomposed to a block diagonal matrix with the *same* format (in terms of the dimension of each block), that matrix representation is called *reducible*, otherwise, it is *irreducible* [65].

An example of an irreducible representation of $\mathbf{C}_3$ is

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R_+ = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon^* \end{pmatrix}, \quad R_- = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix}, \tag{4.16}$$

where $\varepsilon = e^{i\frac{2\pi}{3}}$. The so called *character* table of a group G is a two-dimensional table whose rows indicate the irreducible representations (or *irrep*) of G and its columns indicates the trace of the corresponding matrices. $\mathbf{C}_3$ has three irreducible representations denoted by $\{A, E_+, E_-\}$ and its character table is given in Table 4.3.

$\chi(\mathbf{C}_3)$	$\mathbb{1}$	R_+	R_-
A	1	1	1
E_+	1	ε	ε^*
E_-	1	ε^*	ε

Table 4.3: The character table of $\mathbf{C}_3$.

For a given group G with abstract group elements $g \in G$, and irreducible matrix representations $M_\alpha(g)$, the operator

$$\hat{P}_\alpha = \frac{d_\alpha}{|G|} \sum_g \chi_\alpha(g)\, M_\alpha(g), \tag{4.17}$$

projects a vector (function) ψ into the subspace of the α^{th} *irrep* [66]. Here, d_α is the dimension of the $M_\alpha(g)$ (the dimension of matrices in the α^{th} *irrep*), $|G|$ is the order of the group (the number of group elements), and $\chi_\alpha(g)$ is the character of the α^{th} *irrep* of g.

In case of $\mathbf{C}_3$ group, the normalized projection operators are

$$\begin{aligned} \hat{P}_A &= \frac{1}{3}(\mathbb{1} + R_+ + R_-), \\ \hat{P}_{E_+} &= \frac{1}{3}(\mathbb{1} + \varepsilon\, R_+ + \varepsilon^*\, R_-), \\ \hat{P}_{E_-} &= \frac{1}{3}(\mathbb{1} + \varepsilon^*\, R_+ + \varepsilon\, R_-). \end{aligned} \tag{4.18}$$

As an application of this, one can find the symmetry of any spatial function $f(x,y,z)$ by applying the group projectors on it and see whether it has A symmetry or $E_\pm$ symmetry or a combination of both. For example z has A symmetry and $x-iy$ has E_+ symmetry. The reason is that

$$\begin{aligned} \hat{P}_A.z = z, \qquad & \hat{P}_{E_\pm}.z = 0. \\ \hat{P}_{E_+}.(x-iy) = (x-iy), \qquad & \hat{P}_{E_-}.(x-iy) = 0, \qquad \hat{P}_A.(x-iy) = 0 \end{aligned} \tag{4.19}$$

Now that we are familiar with the $\mathbf{C}_3$ group and its properties, we proceed to the symmetry analysis of the wavefunction of a methyl group.

4.4 The Rovibronic Hamiltonian of a Methyl Group

The total Hamiltonian of a system consisting of N_e electrons and N_n nuclei is

$$H_{\text{tot}} = T_n + T_e + V_{nn} + V_{ee} + V_{ne}, \tag{4.20}$$

where T_n (T_e) is the total kinetic energy of all nuclei (electrons), V_{nn} (V_{ee}) is the sum of all internuclear (interelectron) interactions such as electrostatic repulsions and V_{ne} is the sum of all interactions between nuclei and electrons. The solution to the Schrödinger equation of this group of $N_e + N_n$ particles cannot be written as $\psi_e \otimes \psi_n$ because the interaction term V_{ne} is not negligible. However, since electrons are much lighter than nuclei, an electron is much faster than a nucleus, and thus, its corresponding energy is very larger than the nuclear energy. This justifies the Born-Oppenheimer approximation [67, 68], that is commonly used in the quantum chemistry to effectively separate the wave function into an electron part and a nuclear part. In the first step of this approximation, the nuclear kinetic energy is neglected in comparison with that of the electrons, but the coulomb interaction V_{ne} is not neglected. As a result, one can treat the nuclei at a fixed geometry or in certain configurations in space with a slow motion. Then, solve the Schrödinger equation for the electron wavefunction only, yielding ψ_e which is derived in the nuclear coordinates. In the second step, for each electron state, the nuclear wavefunction is obtained by including an effective potential in the Hamiltonian that serves as a replacement for each electron wavefunction. Indeed, in each electronic level, there is a set of eigenergies for the nuclear spins. The BO approximation reduces the complexity of the computation considerably, specially when the electron wavefunction is mostly in its ground state.

A methyl group consists of a carbon bonded symmetrically to three hydrogen atoms (pyramidal geometry). In the following sections, we study the low temperature spatial motion of a spherical top molecule that has a single methyl group, $X - CH_3$. Here, X can be an atom, such as fluoromethane CH_3F, or a group of atoms, such as ethane C_2H_6. We are interested in the solid phase of $X - CH_3$ molecule, where the translational and external rotation of this *rigid* body or its center of mass is negligible. Excluding the spin degree of freedom, a methyl group has rotation, vibration and electronic degrees of freedom that are known as Rovibronic for short. We analyze the symmetry of the total wavefunction of a methyl group in the following steps: First, we assume the BO approximation is valid and break the rovibronic wavefunction into $\psi_{\text{Rovibronic}} = \psi_e \otimes \psi_n$, and evaluate the symmetry of the electronic wavefunction; Next, we make some justifications to approximate the nuclear spatial wavefunction as a product of the vibrational wavefunction and the internal rotation wavefunction i.e., $\psi_n = \psi_{\text{vib}} \otimes \psi_{\text{rot}}$, and evaluate the symmetry of ψ_{vib}. After that, we explicitly compute the eigenstates and the eigenenergies of the internal rotation Hamiltonian; Finally, when we have a good understanding of the spatial motion of a methyl group, the spin degree of freedom is included and the symmetry of the total wavefunction is discussed.

4.5 The Symmmetry of the Electronic Ground State

At low temperature (solid phase), the external rotational and translational motion are negligible and it is a fair assumption to consider a fixed molecular framework in which the nuclei rotate and/or vibrate near their equilibrium locations relative to a fixed origin (center of mass). Since the nuclear motion is very slow compared to the electron energy scale, it is assumed that the electron cloud *instantly* reforms its shape to follow the nuclear geometry. Therefore, from now on, we consider the BO approximation and analyze the symmetry of the electronic ground state.

Consider a rigid symmetric top molecule $X-CH_3$. The carbon atom, that is located at the centre, makes a covalent bond with each one of the 3 hydrogen atoms as well as a covalent bond with an atom x from the X part of the molecule. We use the Linear Combination of Atomic Orbital (LCAO) method to compute the molecular orbital or the electron wavefunction. A free carbon that is not bonded to any other atom has this orbital configuration

$$\underset{1s}{\uparrow\downarrow}\ \underset{2s}{\uparrow\downarrow}\ \underline{\underset{2p_x}{\uparrow}}\ \underline{\underset{2p_y}{\uparrow}}\ \underline{\underset{2p_z}{\ }} \tag{4.21}$$

But, once the carbon makes covalent bonds in $X-CH_3$, the last 4 electrons in $2s$ orbital and $2p$ orbitals are mixing together to form 4 new *hybrid orbitals* that are ready to share a bond with the other atoms [69]. This is known as *the hybridization of the electronic state* and the hybrid orbitals are represented by sp^3,

$$\underset{1s}{\uparrow\downarrow}\ \underline{\underset{sp^3}{\uparrow}}\ \underline{\underset{sp^3}{\uparrow}}\ \underline{\underset{sp^3}{\uparrow}}\ \underline{\underset{sp^3}{\uparrow}} \tag{4.22}$$

Four symmetrically orthogonal hybrid orbitals are

$$\begin{pmatrix} O_1^{sp^3} \\ O_2^{sp^3} \\ O_3^{sp^3} \\ O_4^{sp^3} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 2s \\ 2p_x \\ 2p_y \\ 2p_z \end{pmatrix}. \tag{4.23}$$

Each of these hybrid orbitals has a large cylindrical head with a positive value, and a small tail with a negative value, and they all together shape a tetrahedron that is demonstrated in Figure 4.2. To obtain the figure we used the solution to the Schrödinger equation for the hydrogen atom with

$\psi_{nlm} = R_{nl}(r)\, Y_l^m(\theta,\phi)$ that results in

$$\begin{aligned} 2s &= R_{20}(r)\, Y_0^0(\theta,\phi), \\ 2p_z &= R_{21}(r)\, Y_1^0(\theta,\phi), \\ 2p_x &= R_{21}(r)\, \frac{1}{\sqrt{2}i}\, \left(Y_1^1(\theta,\phi) + Y_{-1}^1(\theta,\phi)\right), \\ 2p_y &= R_{21}(r)\, \frac{1}{\sqrt{2}}\, \left(Y_1^1(\theta,\phi) - Y_{-1}^1(\theta,\phi)\right), \end{aligned} \tag{4.24}$$

where $Y_l^m(\theta,\phi)$ are the spherical harmonics and R_{nl} is the radial wavefunction.

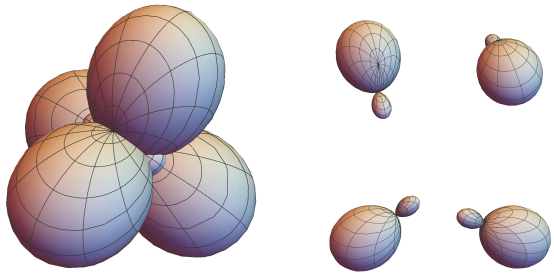

Figure 4.2: Methyl Group Molecular Orbital: Four symmetrically orthogonal hybrid atomic orbitals of the carbon in $X-CH_3$ type molecule form a tetrahedron. Each of these hybrid orbitals contributes in a covalance bond by sharing an electron with a nearby atom. The right picture demonstrates each individual o^{sp^3} orbital.

The hybrid orbitals, O^{sp^3}, represent the carbon's contribution to the molecular orbital. Each of the nearby hydrogen atoms also contributes to the covalent bond by sharing its electron in the $1s$ orbital. Similarly, the X part of the molecule contributes in the 4^{th} bond by sharing its electron in the O_x atomic orbital. According to the LCAO method, the molecule orbital of $X-CH_3$ is a linear combination of the carbon hybrid orbitals, o^{sp^3} and the hydrogen's $1s$ orbital and/or the O_x orbital. It is known that the *bonding* combination has a lower energy than the *anti-bonding* combination [69], therefore, the ground state of the molecular orbital is

$$\psi_e = \sum_{j=1}^{3} \frac{1}{\sqrt{2}} \left(O_j^{sp^3} + 1s_j\right) + \frac{1}{\sqrt{2}} \left(O_4^{sp^3} + O_x\right). \tag{4.25}$$

One can check that this electronic ground state is a totally symmetric function by assuming that O_x is symmetric. Even if O_x is not symmetric, we can still say that the contribution from the

methyl group ($-CH_3$) in the molecular electronic cloud is symmetric. In the future, we use this electronic wavefunction to evaluate the symmetry of the charge density distribution.

4.6 Internal Rotation-Vibration Wave Function

Excluding the spin space, the translational energy, the external rotational energy and the electronic space of a rigid $X-CH_3$ type molecule, the only term that is left in the Hamiltonian is the internal rotation-vibration of the nuclei. In general, the rotation and the vibration are not two independent degrees of freedom, but, we might still be able to treat them separately. The vibrational energies are normally in the order of 1000 cm^{-1}, whereas the rotational energies are in the order of 10 cm^{-1} [69]. Therefore, one can treat the rotational variables as a constant, and solve the Schrödinger equation by considering the vibrational part only. This way, similar to the Born-Oppenheimer approximation, for each vibrational state ν, an effective potential V_ν is added to the rotational part of the Schrödinger equation.

The solution to the vibrational Schrödinger equation for a polyatomic molecule has been studied extensively and its detail is beyond the scope of this thesis [70]. But, for our future analysis, we need to know the symmetry of the vibrational wavefunction at low temperature, and hence, we briefly review the argument in the molecular spectroscopy text books.

Consider the nuclear frame of a polyatomic molecule with N nuclei, where the nuclear center of mass is at the origin of the fixed molecular frame $(\mathbb{X},\mathbb{Y},\mathbb{Z})$. Thus, the Cartesian coordinate of each nucleus is given by $\vec{r}_i=(x_i,y_i,z_i)$ relative to the origin. In a rigid body, a potential $V_{\text{vib}}(\{\Delta\vec{r}_i\})$ confines each uncleus motion near its equilibrium value, where $\Delta\vec{r}_i=\vec{r}_i-\vec{r}_i^{\,eq}=(\Delta x_i,\Delta y_i,\Delta z_i)$ indicates the displacement of the i^{th} uncleus. The vibrational potential can be Taylor expanded in terms of *vibrational normal coordinates*, Q_t, which are defined as a mass weighted linear combination of displacements ($\{\Delta\vec{r}_i\}$) [69]. The first order approximation of the Taylor expansion is

$$V^0_{\text{vib}}=\frac{1}{2}\sum_{t=1}^{3N-6} c_t\, Q_t^2. \tag{4.26}$$

There are $3N-6$ vibrational normal mode because the external translational and rotational motions are excluded. Therefore, up to the first order approximation, the vibrational potential acts like a multi-dimension harmonic oscillator. At low temperature, we can assume that the vibrational wavefunction is in the ground state, which has a Gaussian distribution, and conclude that the vibrational wavefunction is a symmetric function.

In case of methyl groups, the symmetry axis defines the z direction in the molecular frame. At equilibrium, a methyl group has a pyramidal geometry with carbon located at the origin and

three protons located in a plane perpendicular to the symmetry axis, z. Let $(r_j, \theta_j, \varphi_j)$ denote the coordinate of the j^{th} proton relative to the origin. In the *free rotor* limit, when the methyl group is freely rotating around the symmetry axis, φ_j is a random variable but the CH bond's length and angle are almost constant with displacements or vibrations near the equilibrium values. Indeed, considering the pyramidal geometry, $r_j \approx r_0$, $\theta_j \approx \theta_0$ for all $j = 1,2,3$, and $\phi_1 = \phi$, $\phi_2 = \phi + \frac{2\pi}{3}$ and $\phi_3 = \phi - \frac{2\pi}{3}$. Therefore, if we just focus on the motion of the $-CH_3$ part of a symmetric top molecule and neglect the anharmonicity of the vibrational potential, the internal rotation-vibration part of the methyl group's wavefunction is

$$\psi_{\text{rot-vib}} = \psi_{\text{vib}}(\{Q_1, Q_2, ..., Q_6\}) \otimes \psi_{\text{rot}}(\varphi). \tag{4.27}$$

At low temperature, the ground state of vibration, ψ_{vib} appears as as an effective potential, $V_{\text{eff}}(\varphi)$ that influences the internal rotational motion, which is explained in detail in the next section.

4.7 Internal Rotation of a Methyl Group

The internal rotation or the *torsional* degree of freedom of a methyl group has been extensively studied in literature, [71–74]. Idealistically, a methyl group is a *free rotor* that is a rigid body *freely* rotating around the z axis and its Hamiltonian is simply the z component of the total angular momentum,

$$H_{\text{rot}} = \hat{L}_z = \frac{-\hbar^2}{2I_0} \frac{\partial^2}{\partial \varphi^2}, \tag{4.28}$$

where I_0 is the moment of inertia and the angle φ is conventionally defined as the angle between a proton and a reference axis in the molecular framework. The eigenfunctions of this free rotor are $\frac{e^{\pm il\varphi}}{\sqrt{2}}$ with corresponding eigenenergies $E_l = \frac{\hbar^2}{2I_0}\, l^2$ where $l \in \{0, \pm 1, \pm 2, ...\}$. The constant $F = \frac{\hbar^2}{2I_0}$ is also referred as the *free rotor energy* constant.

Realistically, a methyl group in $X - CH_3$ molecule does not rotate freely because of existance of a *hindering* potential which is imposed by the rest of the molecule as well as other external molecules[1]. For example, in ethane the molecule prefers to be in the staggered configuration rather than the eclipsed configuration, [76]. The amount of energy that is required to move from one configuration to another defines the height of the hindering potential or the *barrier* (Figure 4.3). Therefore, in addition to the free rotation term, there is an extra potential that

[1] The main source of hindering potential depends on the molecule. For example in case of ethane van der Waals interactions and hyperconjugation have been reported in literatures [75] and [76].

affects the rotational motion,

$$H_{\text{tor}} = \frac{-\hbar^2}{2I_0}\frac{\partial^2}{\partial\varphi^2} + V_{\text{h}}(\varphi), \tag{4.29}$$

in which

$$V_{\text{h}}(\varphi) = \sum_k \frac{V_k}{2}\left(1-\cos[3k\ \varphi]\right), \quad \text{with} \quad k = 1,2,.... \tag{4.30}$$

Depending on the geometry of the molecule, the hindering potential has 3 fold symmetry, 6 fold

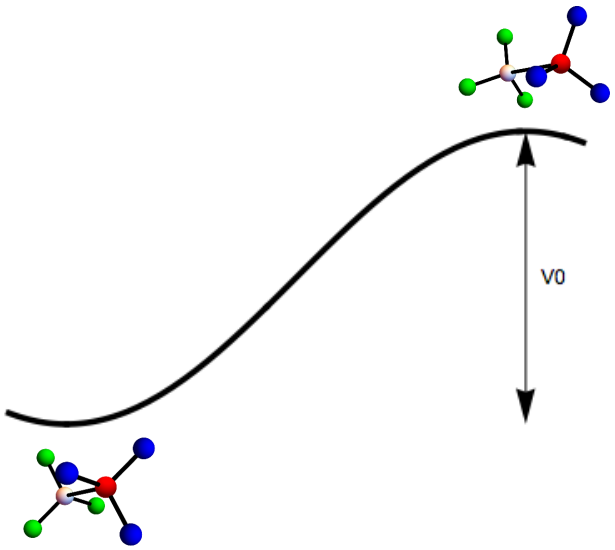

Figure 4.3: Ethane Hindering Potential: The barrier height is the amount of energy that is required to move from the staggered configuration to the eclipsed configuration.

symmetry and etc. But, often the first term $V_3 = V_0$ is the dominant one and all other $V_{3k\neq 3}$ are negligible. For the following discussion we consider a 3-fold potential only.

In the *extreme rigid rotor* limit or *the high barrier potential*, the motion along the φ direction is also very restricted, because, the barrier height is much larger than the free rotor energy, i.e., $V_0 \gg F$. Thus, we approximate $V(\varphi)$ with three quantum wells and treat each well like a harmonic potential,

$$V_{\text{h}} \approxeq \frac{V_0}{2}\left(1-\cos[3\ \varphi]\right) \approxeq \frac{V_0}{2}\left(\frac{(3\varphi)^2}{2!} - \frac{(3\varphi)^4}{4!} + ...\right). \tag{4.31}$$

Reasonably, each level has the degeneracy of 3, because there are three wells, and so, three harmonic oscillators. The corresponding 3-fold degenerate eigenenergies are $E_n \approxeq 3\sqrt{\frac{V_0}{I_0}}(n+\frac{1}{2})$ with $n = 0,1,2,...$

In non-extreme cases, where the methyl group is neither a free rotor nor an extreme rigid rotor (harmonic oscillator), we solve the Schödinger equation numerically and plot the eigenenergies as a function of a parameter $0 < q < 1$, where the $q = 0$ corresponds to a free rotor ($V_0 = 0$) and the $q = 1$ corresponds to an extreme rigid rotor ($V_0 \gg F$). The first tweleve eigenenergies of a methyl group ranging from the free rotor limit to the extreme rigid rotor limit are demonstrated in Figure 4.4. The left plot is associated with the nearly free rotor ($V_0 \approx 0$), and as expected, other than the ground state ($l = 0$), all other energy levels are double degenerate. At an intermediate regime, when $V_0 \geq F$, every three energy levels tend to group together and form a *band* that consists of a non-degenerate level and a double degenerate level. Thus, at $V_0 \geq F$ limit we label the internal rotation eigenstates with $\Phi_{\lambda,n}$ with corresponding energies $E_{\lambda,n}$ in which n refers to the band level (harmonic oscillator level) and $\lambda \in \{0, \pm 1\}$. At each band n, we denote the *internal* energy difference between the $\lambda = 0$ level and the $\lambda = \pm 1$ levels with ΔE_n. At specific q, we observe that the sign of the energy *splitting*, ΔE_n, changes from the n^{th} band to the $(n+1)^{\text{th}}$ band, and its amplitude gets larger and larger as we go higher in n. Because of these two observations, it is reasonable to see at some point the $E_{\lambda=0,n}$ level and $E_{\lambda=0,n+1}$ merge together and form a double degenerate level. Indeed, even in the intermediate regime where $V_0 \geq F$, the high energy levels behave like that of a free rotor and are doubly degenerate. Because in that energy scale, the methyl group effectively *does not see* the barrier. These numerical observations are better justified in the upcoming section. For larger q (or larger barrier height), the internal splitting ΔE_n gets smaller and smaller and eventually it becomes zero at the extreme rigid rotor limit, yielding to 3-fold degenerate levels. The right plot of Figure 4.4 is associated with the nearly extreme rigid rotor ($V_0 \gg F$).

Each molecule has a certain geometry and mass, and so, has a certain free rotation energy, F. It also has an associated hindering potential with specific barrier heigh, V_0. Thus, depending on the ratio $\frac{V_0}{F}$, an organic compound may be considered as a free rotor, or an intermediate rotor, or an extreme rigid rotor based on the structure of the lowest energy levels. Table 4.4 lists some examples of chemical compounds with their corresponding barrier heights, free rotor energy constant and the splitting of the ground state $n = 0$.

4.7.1 The Symmetry of the Torsional States

A methyl group forms a $\mathbf{C}_3$ group in the spatial space that has three irreducible representations, $\{A, E_+, E_-\}$, with their corresponding character values $\{1, \varepsilon, \varepsilon^*\}$ with $\varepsilon = e^{i\frac{2\pi}{3}}$. In previous section, we solved the Schrödinger equation numerically, yielding the torsional eigenfunctions $\Phi_{\lambda,n}(\varphi)$ in the intermediate rigid rotor limit ($V_0 \geq F$). Here, we analyze the symmetry of $\Phi_{\lambda,n}(\varphi)$, and show that the label λ is associated to one of the irreducible representations of $\mathbf{C}_3$ group.

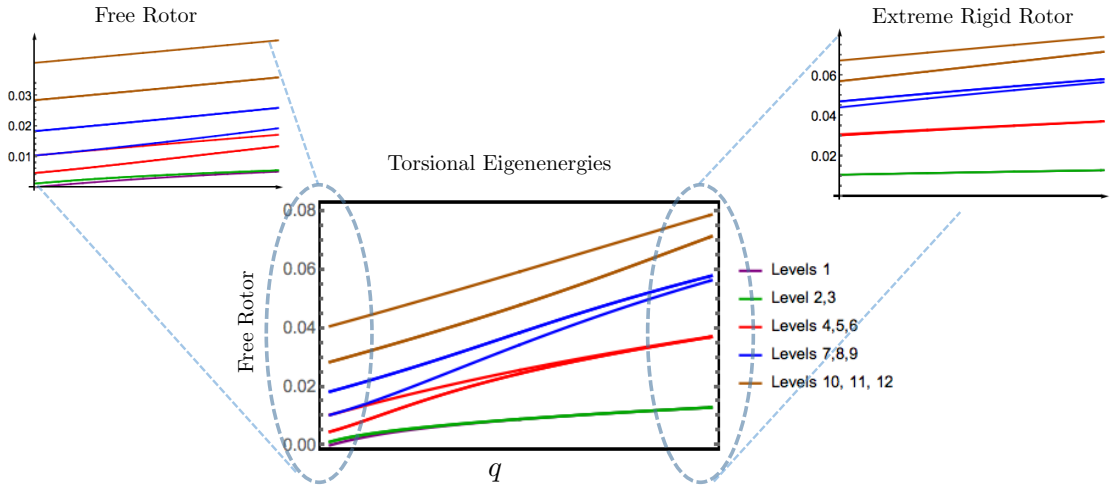

Figure 4.4: Torsional Eigenenergies of a Methyl Group: The left side, $q = 0$, is the free rotor limit when the hindering potential is very shallow or nearly zero and the right side, $q = 1$, is the extreme rigid rotor when the barrier height is very large compared to the free rotor energy.

We expand $\Phi_{\lambda,n}$ in terms of free rotor eigenfunctions which form an orthonormal basis,

$$\Phi_{\lambda,n}(\varphi) = \sum_l c_l \frac{e^{il\varphi}}{\sqrt{2}}. \tag{4.32}$$

If an eigenfunction Φ has *A symmetry*, it must be invariant under the $\frac{2\pi}{3}$ rotation. Therefore, the non-zero terms in the above expansion must be $l = 3\,k$, where k is an integer. Similarly, if it has $E_\pm$ *symmetry*, under the $\frac{2\pi}{3}$ rotation it must pick up a phase $e^{\pm i\frac{2\pi}{3}}$, i.e., $\Phi_{\lambda,n}(\varphi \pm \frac{2\pi}{3}) = e^{\pm i\frac{2\pi}{3}}\,\Phi_{\lambda,n}(\varphi)$. Therefore, the non-zero terms in the above expansion must be $l = 3\,k+1$ for E_+ symmetry and $l = 3\,k-1$ for E_- symmetry. This property can be used as a test to see which kind of symmetry each numerical eigenfunction has, A or $E_\pm$ or a combination. We realize that in n^{th} harmonic oscillator level, the $\lambda = 0$ state has only A symmetry and the the doubly degenerate states, $\lambda = \pm 1$, have $E_\pm$ symmetry. Because $E_\pm$ are degenerate, any superposition of them is a solution to the Schrödinger equation. The first 6 numerical eigenfunctions of the torsional Hamiltonian are plotted in Figure 4.5 for the choice of $V_0 = 32$ meV and $F = 0.6$ meV.

An alternative approach for finding the torsional eigenfunctions is to treat $V_{\text{h}}(\varphi)$ as a periodic lattice with three wells. According to the Bloch theorem [83], given a periodic potential $V(x)$ with N wells (atoms), the lattice (or the molecule) wavefunction, $\Phi(x)$, has the following

Compound	$V_0(meV)$	$F(meV)$	$\Delta E_0(GHz)$	Ref	Regime
o-fluorotoluene	28.14	0.64	20	[77]	Intermediate
m-fluorotoluene	2.6	0.66	860	[78]	Free Rotor
Lithium acetate			60	[79]	
4-Methylpyridine	7.3		120	[80]	Intermediate
o-toluidine	86.79	0.66	350	[81] , [82]	Intermediate

Table 4.4: Examples of chemical compounds with their corresponding barrier height and free rotor energy. The ΔE_0 in the third column is the energy splitting between $(\lambda = \pm 1, n = 0)$ and $(\lambda = 0, n = 0)$ levels of the torsional states (or the splitting between $l = 0$ and $l = \pm$ levels of the rotational states, in the limit of the free rotor).

properties:

$$\begin{aligned} \Phi(x+a) &= e^{i\kappa a}\Phi(x), \\ \Phi(x+Na) &= \Phi(x), \end{aligned} \tag{4.33}$$

where a is the distance between two adjacent wells (lattice constant) and $\kappa = \lambda \frac{2\pi}{Na}$ is the pseudo-momentum with $\lambda = 0, \pm 1, \pm 2, \ldots$. Using the Bloch theorem and the LCAO method with no hybridization assumption, the lattice wave function of the n^{th} energy level is $\Phi_n(x) = \sum_{j=1}^{N} e^{ikaj}\chi_n^{(j)}(x)$ in which $\chi(x)$ is the solution of each atom.

The 3-fold symmetry potential that hinders the methyl group's rotation around the symmetry axis is also considered as $N = 3$ periodic lattice with the lattice constant $a = \frac{2\pi}{3}$. Therefore, we take the Bloch periodic wavefunction and simply replace $x = \varphi$ to get

$$\Phi_{\lambda,n}(\varphi) = \sum_{j=1}^{3} e^{i\frac{2\pi}{3}\lambda j}\chi_n^{(j)}(\varphi), \tag{4.34}$$

in which $\chi_n^{(j)}$ is the n^{th} eigenfunction of the j^{th} well (harmonic oscillator). The boundary condition, $\Phi(\varphi + 2\pi) = \Phi(\varphi)$, results in $\lambda = 0, \pm 1$. Thus,

$$\begin{aligned} \Phi_{\lambda=0,n} &= \frac{1}{\sqrt{3}}\left(\chi_n^{(1)} + \chi_n^{(2)} + \chi_n^{(3)}\right), \\ \Phi_{\lambda=1,n} &= \frac{1}{\sqrt{3}}\left(\chi_n^{(1)} + \varepsilon^*\,\chi_n^{(2)} + \varepsilon\,\chi_n^{(3)}\right), \\ \Phi_{\lambda=-1,n} &= \frac{1}{\sqrt{3}}\left(\chi_n^{(1)} + \varepsilon\,\chi_n^{(2)} + \varepsilon^*\,\chi_n^{(3)}\right), \end{aligned} \tag{4.35}$$

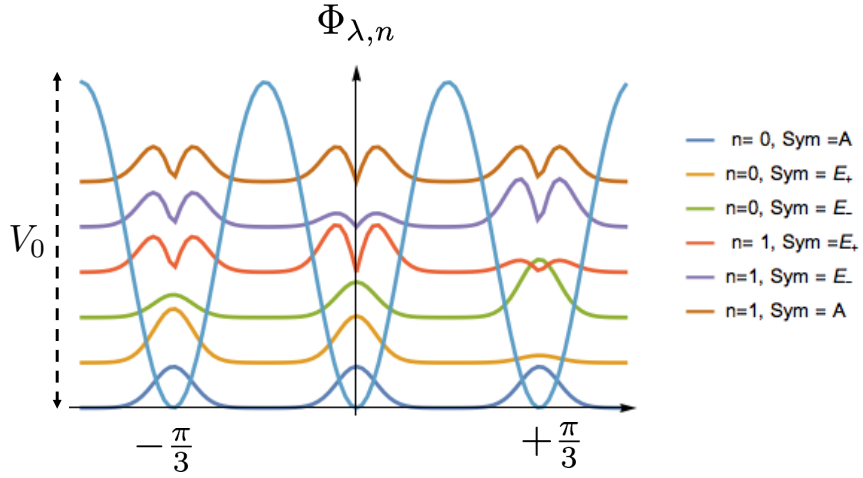

Figure 4.5: Torsional Eigenfunctions: The first 6 eigenfunctions of the torsional Hamiltonian are presented. The first and sixth levels are totally symmetric (A) and the rest have $E_\pm$ symmetry.

with $\varepsilon = e^{i\frac{2\pi}{3}}$. Because of the cyclic boundary condition, we have $\chi^j(\varphi + \frac{2\pi}{3}) = \chi^{j+1}(\varphi)$. Consequently, the $\lambda = 0$ state has A symmetry and the $\lambda = \pm 1$ states have $E_\pm$ symmetry. We should also note that the above LCAO expansions are valid in the limit of no-hybridization assumption where the overlap between $\chi_n^{(j)}$ and $\chi_{n+1}^{(j')}$ is negligible. In that limit, the Hamiltonian is block diagonal and the corresponding Schrödinger equation for the n^{th} block is

$$\begin{aligned} H_n\,\Phi_{\lambda,n} &= E_{\lambda,n}\,\Phi_{\lambda,n} \\ \begin{pmatrix} \alpha_n & \beta_n & \beta_n \\ \beta_n & \alpha_n & \beta_n \\ \beta_n & \beta_n & \alpha_n \end{pmatrix} \begin{pmatrix} 1 \\ e^{\frac{2\pi i}{3}\lambda} \\ e^{-\frac{2\pi i}{3}\lambda} \end{pmatrix} &= E_{\lambda,n} \begin{pmatrix} 1 \\ e^{\frac{2\pi i}{3}\lambda} \\ e^{-\frac{2\pi i}{3}\lambda} \end{pmatrix} \\ \Longrightarrow E_{\lambda,n} &= \alpha_n + 2\beta_n \cos\left(\frac{2\pi}{3}\lambda\right). \end{aligned} \tag{4.36}$$

Here, $\alpha_n = E_n^{(0)}$ is the eigenenergy of each well and $\beta_n = -E_n^{(0)}\langle \Phi_n^{(j)} | \Phi_n^{(j+1)} \rangle$ is the overlap between the wavefunctions of the two adjacent wells. This overlap results in a splitting $|\Delta E_n| = 3\beta_n$ between the A symmetry level and the $E_\pm$ symmetry levels. This is an analogy to the energy band gap in the solid state physics when we deal with a periodic lattice with large N.

The overlap between the wavefunctions of two wells provides a qualitative and yet informative description of the torsional eigenenergies. The symmetry of each well/harmonic oscillator's wavefunctions changes from the n^{th} level to the $(n+1)^{\text{th}}$ level. Consequently, the sign of the

overlap, β_n, or the splitting ΔE_n changes from the n^{th} level to the $(n+1)^{\text{th}}$ level, and accordingly the ordering between the A level and the $E_\pm$ levels changes. Moreover, in high energy levels, the wavefunction is less confined within a well and therefore its overlap with the neighbour's wavefunction is larger. This means, as we go higher and higher in energy, the splitting between A symmetry and $E_\pm$ symmetry gets larger and larger and at some point the labelling $\{A, E_\pm\}$ is not valid any more, because, the no-hybridization assumption breaks. Indeed, if the torsional energy is high enough, the barrier is not effective any more and the methyl group behaves like a free rotor. This symmetry analysis is consistent with the numerical result presented previously.

4.8 The Spin Hamiltonian of a Methyl Group

So far, we have not considered the spin degree of freedom, which is the subject of this section. In the presence of a magnetic field and in the absence of any chemical shift anisotropy (CSA) and/or any dipole-dipole interaction (DD), the spin Hamiltonian of the three protons in a methyl group is

$$H_{\text{spin}} = \frac{\omega_h}{2} \sum_{i=1}^{3} \sigma_z^{(i)} + 2\pi J_0 \sum_{j<k} \vec{\sigma}^{(j)}.\vec{\sigma}^{(k)}, \tag{4.37}$$

where $\omega_h = \gamma_h B_0$ is the proton frequency and J_0 is the scalar coupling constant between any two protons, which is normally small compared to the Zeeman energies. In the absence of CSA and DD interactions, these protons are indistinguishable and they form a $\mathbf{C}_3$ group. This means that the spin eigenstates are invariant under the cyclic permutation operator, that is defined by

$$\begin{aligned} \hat{P}_+ |i\rangle \otimes |j\rangle \otimes |k\rangle &= |k\rangle \otimes |i\rangle \otimes |j\rangle, \\ \hat{P}_- |i\rangle \otimes |j\rangle \otimes |k\rangle &= |j\rangle \otimes |k\rangle \otimes |i\rangle, \end{aligned} \tag{4.38}$$

for $\forall |ijk\rangle \in \mathfrak{B}_c(\mathscr{H}_{1/2}^{\otimes 3})$. It is straightforward to find a matrix representation of $\hat{P}_\pm$ and expand it in the Pauli operator basis,

$$\hat{P}_\pm = \frac{1}{4}\left(\mathbb{1} + \vec{\sigma}^{(1)}.\vec{\sigma}^{(2)} + \vec{\sigma}^{(2)}.\vec{\sigma}^{(3)} + \vec{\sigma}^{(1)}.\vec{\sigma}^{(3)} \mp i \sum_{\alpha\beta\gamma} \varepsilon_{\alpha\beta\gamma}\, \sigma_\alpha \otimes \sigma_\beta \otimes \sigma_\gamma \right), \tag{4.39}$$

where $\varepsilon_{\alpha\beta\gamma}$ is the Levi-Civita coefficient with $\alpha, \beta, \gamma \in \{x, y, z\}$. The complex eigenvalues of the $\hat{P}$ are $\{1, \varepsilon, \varepsilon^*\}$ with $\varepsilon = e^{2\pi i/3}$ that correspond to three irreducible representations $\{A, E_+, E_-\}$ respectively. We represent the eigenstates of $\hat{P}_+$ with $|s, g_s\rangle$ where the s indicates the symmetry irreducible representations, $s \in \{A, E_+, E_-\}$, and the g_s is a label to distinguish the degenerate states within each symmetry subspace. Indeed, $g_A \in \{1, 2, 3, 4\}$ and $g_{E_\pm} \in \{1, 2\}$. We name

$\{|s,g_s\rangle\}$ the Cyclic Permutation Invariant Basis (CPI basis). One can alternatively label the CPI eigenstates with $|s,m\rangle$ where m is the eigenvalue of $\hat{\mathbf{S}}_z = \frac{1}{2}\sum_{i=1}^{3}\sigma_z^{(i)}$, because, the Zeeman Hamiltonian that is proportional to $\hat{\mathbf{S}}_z$ is diagonal in the CPI basis. The explicit expansion of the CPI basis in terms of the computational basis is given in Table 4.5. Note that the Hilbert space is a direct sum of two subspaces, $\mathscr{H} = \mathscr{H}_A \oplus \mathscr{H}_E$, and each subspace is further decomposed into a product of the symmetry label s and the magnetization label m, i.e., $\mathscr{H}_A = \mathbb{C}^1 \otimes \mathbb{C}^4$ and $\mathscr{H}_E = \mathbb{C}^2 \otimes \mathbb{C}^2$.

$\|s,m\rangle$	Expansion in $\mathfrak{B}_c(\mathscr{H}_{1/2}^{\otimes 3})$	$\hat{P}_+$'s Eigenvalue	$\hat{S}_z$ Eigenvalue
$\|A,3/2\rangle$	$\|\uparrow\uparrow\uparrow\rangle$	1	3/2
$\|A,1/2\rangle$	$\frac{1}{\sqrt{3}}(\|\uparrow\uparrow\downarrow\rangle + \|\downarrow\uparrow\uparrow\rangle + \|\uparrow\downarrow\uparrow\rangle)$	1	1/2
$\|A,-1/2\rangle$	$\frac{1}{\sqrt{3}}(\|\downarrow\downarrow\uparrow\rangle + \|\uparrow\downarrow\downarrow\rangle + \|\downarrow\uparrow\downarrow\rangle)$	1	-1/2
$\|A,-3/2\rangle$	$\|\downarrow\downarrow\downarrow\rangle$	1	-3/2
$\|E_+,1/2\rangle$	$\frac{1}{\sqrt{3}}(\|\uparrow\uparrow\downarrow\rangle + \varepsilon^*\|\downarrow\uparrow\uparrow\rangle + \varepsilon\|\uparrow\downarrow\uparrow\rangle)$	ε	1/2
$\|E_+,-1/2\rangle$	$\frac{1}{\sqrt{3}}(\|\downarrow\downarrow\uparrow\rangle + \varepsilon^*\|\uparrow\downarrow\downarrow\rangle + \varepsilon\|\downarrow\uparrow\downarrow\rangle)$	ε	-1/2
$\|E_-,1/2\rangle$	$\frac{1}{\sqrt{3}}(\|\uparrow\uparrow\downarrow\rangle + \varepsilon\|\downarrow\uparrow\uparrow\rangle + \varepsilon^*\|\uparrow\downarrow\uparrow\rangle)$	ε^*	1/2
$\|E_-,-1/2\rangle$	$\frac{1}{\sqrt{3}}(\|\downarrow\downarrow\uparrow\rangle + \varepsilon\|\uparrow\downarrow\downarrow\rangle + \varepsilon^*\|\downarrow\uparrow\downarrow\rangle)$	ε^*	-1/2

Table 4.5: The cyclic permutation invariant basis expanded in the computational basis.

Note that the spin Hamiltonian in Equation 4.37, does not distinguish these identical protons, and thus, $[H_{\text{spin}}, \hat{P}_\pm] = 0$. This commutation relation does not necessarily imply that spin Hamiltonian and the cyclic permutation operator share an eigenbasis because of the degeneracy. However, it does imply that H_{spin} preserves the symmetry label, s, as it is shown in the following, and so, the eigenstates of the spin Hamiltonian are represented by $\psi_{s,m} \in \text{Span}\{|s,g_s\rangle\}$.

In the CPI basis, all components of the total spin angular momentum, $\hat{\mathbf{S}}_\alpha$ with $\alpha \in \{x,y,z\}$, are indeed block diagonal,

$$\hat{\mathbf{S}}_\alpha = \sum_{m,m'=-\frac{3}{2}}^{\frac{3}{2}} a_{mm'}\,|A,m\rangle\langle A,m'| + \sum_{m,m'=-\frac{1}{2}}^{\frac{1}{2}} b_{mm'}\left(\,|E_+,m\rangle\langle E_+,m'| + |E_-,m\rangle\langle E_-,m'|\right). \quad (4.40)$$

Being block diagonal shows that the symmetry label is *preserved* by the collective spin operators. Considering an interaction noise model where the methyl group interacts symmetrically with the environment via Equation 4.1, and in the absence of the DD couplings and/or the CSA in the system, neither the environment nor the local spin Hamiltonian in Equation 4.37 breaks the cyclic

permutation symmetry. Under these conditions, the symmetry degree of freedom is *protected* against all collective noise, and hence, is a candidate for storing information. Section 4.10 is devoted to a discussion about initializing protected states in the spin degree of freedom of the group of three protons in a methyl group.

Now that we have some understanding of the spin symmetry, the torsional symmetry and the symmetry of the vibrational and the electronic wavefunctions respectively, we proceed to the argument of the symmetry of the total wavefunction and the correlation between the spatial space and the spin space. One may take advantage of this correlation to create a protected state.

4.9 The symmetry of the Total Wavefunction

Considering the approximations we made in previous sections, the electronic, the vibrational, the rotational and the spin degrees of freedom are treated independently and the total wave function is written as a product of them,

$$\Psi_{\text{tot}} = \psi_e \otimes \psi_{\text{vib}} \otimes \psi_{\text{tor}} \otimes \psi_{\text{spin}}. \tag{4.41}$$

In addition, we discussed that at low temperature, ψ_e and ψ_{vib} are symmetric wavefunctions. Thus, the symmetry of the total wavefunction is determined by the symmetry of the product of the internal rotation (torsional) eigenfunctions and the the spin eigenstates.

For both fermionic and bosonic systems, the total wavefunction of three identical particles must be invariant under the $2\pi/3$ rotation, because this rotation is equivalent to two particle exchanges: First, the j^{th} particle with the $(j+1)^{\text{th}}$ one, and second the $(j+1)^{\text{th}}$ particle with the $(j-1)^{\text{th}}$ one, for all $j \in \{1,2,3\}$. This invariance under the rotation narrows the allowed combinations of the torsional eigenfunctions and the spin eigenstates to those that satisfy

$$\text{Sym}(\psi_{\text{tor}}) \times \text{Sym}(\psi_{\text{spin}}) = A,$$

where $\text{Sym}(f)$ stands for the symmetry of f. Thus, the allowed combinations are $A \times A$, $E_+ \times E_-$ and $E_- \times E_+$. Moreover, for a fermionic system, the total wavefunction must not only be symmetric under the rotation but also be antisymmetric under the exchange of any pairs of particles. We apply these rules to the case of a free rotor in the presence of a magnetic field, where the rotational eigenfunctions are $\frac{1}{\sqrt{2\pi}} e^{il\varphi}$ with $l = 0, \pm 1, \ldots$ and the spin eigenstates are $\psi_{s,m}$.

Note that exchanging any pairs of protons leads to $l \to -l$. In case of $\psi_{A,m}$, the spin eigenstates are totally symmetric and therefore the corresponding symmetric rotational eigenfunctions that satisfy $A \times A$ condition, are $\frac{1}{\sqrt{2\pi}} e^{\pm i3k\varphi}$ with k being an integer. In case of $\psi_{E_\pm,m}$, the spin

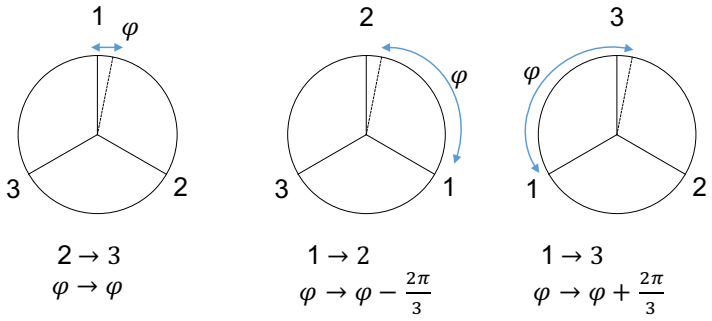

Figure 4.6: Exchange of Two Protons in a Methyl Group: For the exchange of any pair, the permutation cycle changes from 123 to 132, so, $l \to -l$. If we exchange $2 \leftrightarrow 3$, the angle φ is unchanged, otherwise $\varphi \to \varphi \pm \frac{2\pi}{3}$.

eigenstates are neither symmetric nor anti-symmetric and the corresponding rotational eigenfunctions that satisfy $E_\pm \times E_\mp$ conditions, are $e^{i(3k\mp1)\varphi}$, which have $E_\mp$ symmetry under rotation. There is a delicate point here. Depending on which pair of protons are exchanged, the phase of the rotational eigenfunctions and/or the spin eigenstate with symmetries $E_\pm$ varies differently. Without loss of generality, let conventionally define φ to be the angle between the first proton and a fixed axes in the space, Figure 4.6. Under the exchange of $2 \leftrightarrow 3$, φ does not change but under the exchange of $1 \leftrightarrow 3$, $\varphi \to \varphi + \frac{2\pi}{3}$. This is illustrated in Figure 4.6. Correspondingly, the rotational eigenfunctions and the spin eigenstates pick up different phases that are listed in Table 4.6.

Particle Exchange	Rotational Wavefunction	Spin Eigenstate
$2 \leftrightarrow 3$	$e^{il\varphi} \to e^{-il\varphi}$	$\psi_{E_-,m} \to \psi_{E_+,m}$
$1 \leftrightarrow 2$	$e^{il\varphi} \to e^{-il(\varphi+2\pi/3)}$	$\psi_{E_-,m} \to e^{i2\pi/3}\psi_{E_+,m}$
$1 \leftrightarrow 3$	$e^{il\varphi} \to e^{-il(\varphi-2\pi/3)}$	$\psi_{E_-,m} \to e^{-i2\pi/3}\psi_{E_+,m}$

Table 4.6: The phase of the rotational eigenfunctions and the spin eigenstate varies differently depending on which pair of protons are exchanged. To obtain the spin part of this table we used the explicit expansion of $|s,m\rangle$ in terms of the computational basis that was presented in Table 4.5.

Taking into account the above points, the anti-symmetric total wavefunction is

$$\Psi_{\text{tot}} = \begin{cases} \frac{1}{\sqrt{2}}\left(e^{il\varphi} - e^{-il\varphi}\right) \otimes \psi_{A,m}, & l = 3k, \\ \frac{1}{\sqrt{2}}\left(e^{il\varphi} \otimes \psi_{E_{\mp},m} - e^{-il\varphi} \otimes \psi_{E_{\pm},m}\right), & l = 3k \pm 1. \end{cases} \tag{4.42}$$

What is common between $A \times A$ combination and $E_{\pm} \times E_{\mp}$ combinations is that the wavefunction is a difference of two terms and particle exchange swaps them. Interestingly, the two terms are degenerate and orthogonal to each other.

It is straightforward to extend the above argument to an intermediate rigid rotor, where the 3-fold hindering potential barrier height is larger than the methyl group's free rotation energy. In that case, the torsional eigenfunctions are labelled as $\Phi_{\lambda,n}$ where n refers to the n^{th} harmonic oscillator level and λ refers to the rotational symmetry, $\lambda \in \{A, E_{\pm}\}$. In Section 4.7, we showed that for all values of n, the $\Phi_{\lambda,n}$ is a linear combination of the free rotor's eigenfunctions with the same symmetry. As a result, the antisymmetric wave function of an intermediate rigid rotor is simply a linear combination of the antisymmetric wave function of a free rotor that was discussed above. Although, this generalization from the free rotor to an intermediate rigid rotor sounds straightforward, an implicit approximation is considered. When a methyl groups is rotating in the presence of a hindering potential, the three protons are no longer perfectly indistinguishable to the environment, and hence, the spin Hamiltonian Equation 4.37 and corresponding spin eigenstates are an approximation.

4.10 Protected State in Methyl Group

Now that we analyzed the eigenenergies and the eigenstates of a rigid rotor and discussed the symmetry induced coupling between the spin space and the torsional space, we are ready to explore the possibility of initializing a protected state, or perhaps a logical qubit in the collective spin degree of freedom of three identical protons.

4.10.1 Long Lived State by Thermal Means

A protected state is either a classical state (probabilistic mixture of eigenstates) or a quantum state (with non-zero coherence terms). The *Long Lived State* that has been experimentally studied in methyl groups by [73, 79, 84] is an example of a classical protected state. In the following, we review how an LLS in a methyl group can be implemented just by thermal means and discuss why this state is not capable of storing quantum information.

First, let us define the *Long Lived State*. We define *symmetry polarized* states as a set of mixed states that are individually polarized in terms of the symmetry label, but yet are totally mixed in terms of the total magnetization label. They are denoted by $\rho_{A/E_\pm}$, and are given by

$$\begin{aligned}
\rho_A &:= \frac{1}{4}\sum_{m=-\frac{3}{2}}^{\frac{3}{2}} |A,m\rangle\langle A,m| = \frac{1}{4}\left(\begin{array}{c|c} \mathbb{1}_4 & 0 \\ \hline 0 & 0 \end{array}\right), \\
\rho_{E_+} &:= \frac{1}{2}\sum_{m=-\frac{1}{2}}^{\frac{1}{2}} |E_+,m\rangle\langle E_+,m| = \frac{1}{2}\left(\begin{array}{c|cc} 0 & \multicolumn{2}{c}{0} \\ \hline 0 & \mathbb{1}_2 & 0 \\ \hline & 0 & 0 \end{array}\right), \\
\rho_{E_-} &:= \frac{1}{2}\sum_{m=-\frac{1}{2}}^{\frac{1}{2}} |E_-,m\rangle\langle E_-,m| = \frac{1}{2}\left(\begin{array}{c|cc} 0 & \multicolumn{2}{c}{0} \\ \hline 0 & 0 & 0 \\ \hline & 0 & \mathbb{1}_2 \end{array}\right).
\end{aligned} \tag{4.43}$$

An LLS is $\gamma-$polarized in terms of the symmetry label if there is an imbalance of population between the A subspace and the E subspace, and is given by

$$\begin{aligned}
Q_{LLS} &= \frac{(1+\gamma)}{2}\rho_A + \frac{(1-\gamma)}{2}\rho_E \\
&= \frac{1}{8}(\mathbb{1} + \frac{\gamma}{3}\,(\vec{\sigma}^{(1)}.\vec{\sigma}^{(2)} + \vec{\sigma}^{(2)}.\vec{\sigma}^{(3)} + \vec{\sigma}^{(1)}.\vec{\sigma}^{(3)})),
\end{aligned} \tag{4.44}$$

where $\rho_E = \frac{1}{2}\left(\rho_{E_+} + \rho_{E_-}\right)$. Because of the scalar terms $\vec{\sigma}.\vec{\sigma}$ that are invariant under $\hat{\mathbf{S}}_\alpha$, with $\alpha \in \{x,y,z\}$, the Q_{LLS} is protected against all collective noise. The appearance of a scalar term here is similar to the argument of LLS for two spins via the singlet state in Equation 4.5.

Second, we show how to populate Q_{LLS} by thermally cooling a methyl group. Consider an intermediate rigid rotor in the presence of a magnetic field which has torsional eigenfunctions $\Phi_{\lambda,n}$ and spin eigenstates $\psi_{s,m}$. As discussed in section 4.9, for a fermionic system, the product of $\Phi_{\lambda,n} \otimes \psi_{s,m}$ must be symmetric under the $\frac{2\pi}{3}$ rotation, which narrows the allowed combinations of the torsional eigenfunctions and the spin eigenstates to those with symmetry labels $\lambda \times s \in \{A \times A,\ E_\pm \times E_\mp\}$. This can be considered as a sort of *symmetry correlation* between the spatial space and the spin space. One can take advantage of this correlation to initialize the methyl group in a LLS just by cooling.

At relatively low field, when the Zeeman splitting, $\gamma_h B_0$, is negligible compared to the torsional ground state splitting, ΔE_0, the spatial Hamiltonian is dominant. Figure 4.7 schematically represents the energy diagram of the first ground state of a methyl group with a medium rotational barrier, in which ΔE_0 is the splitting between the $(\lambda = A, n = 0)$ level and the $(\lambda = E_\pm, n = 0)$

levels. At relatively low temperature, when the methyl group is cooled much below the torsional ground state splitting, $k_BT \ll \Delta E_0$, the $(\lambda = A, n = 0)$ level in the torsional space is highly populated. If this temperature is still high compared to the Zeeman splitting, the (s, m) levels in the spin space are almost equally populated and the spin density matrix is almost equal to an identity in terms of the spin magnetization label (Equation 4.43).

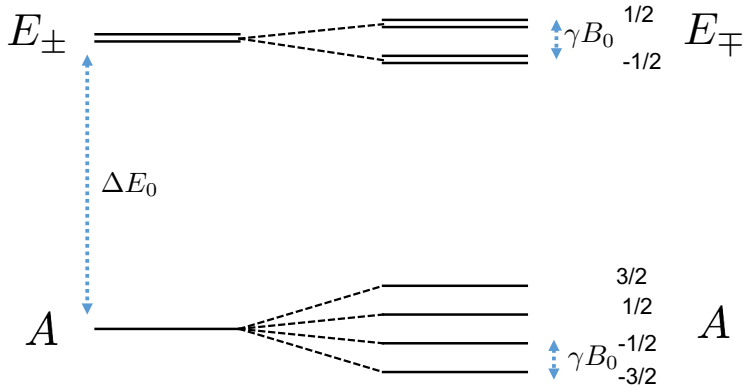

Figure 4.7: Eigenenergies of a Rigid Rotor with Medium Barrier Height: Each torsional level with symmetry λ is further split to more energy levels with spin symmetry s, such that the total symmetry is $\lambda \times s = A$. ΔE_0 is the splitting between the $(\lambda = A, n = 0)$ level and the $(\lambda = E_\pm, n = 0)$ levels on the torsional space.

Thus, at low field and low temperature ($\gamma B_0 \ll k_bT \ll \Delta E_0$), according to the Boltzmann distribution, there is a significant population imbalance between the $\Phi_{A,n=0}$ and the $\Phi_{E_\pm,n=0}$ in the torsional space. Consequently, due to the spin-space symmetry correlation, there is an imbalance of population imbalance the ρ_A and the ρ_E in the spin space. As a result, this thermal process corresponds to initializing the collective spin state of a methyl group in a γ-polarized long lived state, Q_{LLS} with $\gamma = \tanh[\Delta E_0/k_bT]$. This has been experimentally demonstrated in [73, 79, 84].

Note that the Q_{LLS} that was introduced in Equation 4.44 is a classical mixture of ρ_A and ρ_E, which are themselves mixed states. When neither the local spin Hamiltonian nor the interaction Hamiltonians distinguishes spin, one is not able to create coherence between the A subspace and the E subspace, and use $\{A/E\}$ as a logical basis for quantum information processing. In other words, the spin Hamiltonians have a block diagonal form when spins are indistinguishable, and hence, the Hilbert space is a direct sum of the two subspaces, $\mathscr{H} = \mathscr{H}_A \oplus \mathscr{H}_E$. But, the subspace $\mathscr{H}_E$ alone can be used for encoding a logical qubit, which is the subject of discussion in the next section.

4.10.2 Protected State via the Electromagnetic Field Interaction

As mentioned before, the E subspace of three identical protons is decomposed into a product of two subsystems, $\mathscr{H}_E = \mathbb{C}^2 \otimes \mathbb{C}^2$, where the first subsystem refers to the $E_\pm$ symmetry and the second subsystem refers to the total magnetization $m \in \{\pm\frac{1}{2}\}$. Mathematically speaking and according to Section 4.2.3, the $E_\pm$ subsystem of the spin space can be used for encoding quantum information, since the logical basis states are well defined in that noiseless subsystem. But, there is a delicate point here that prevents us from doing so. On one hand, the protection against collective noise has its roots in the indistinguishably of spins which allows us to consider the symmetry label E_+/E_- as a noiseless subsystem. On the other hand, if neither the the local spin Hamiltonian in Equation 4.37 nor the coupling to the environment in Equation 4.1 distinguishes spins, the spin eigenstates $\psi_{E_+,m}$ and $\psi_{E_-,m}$ are degenerate, and thus, the logical basis $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are not accessible individually. When the logical basis states are not individually accessible, implementing any arbitrary logical qubit is not feasible. We emphasize here that when the methyl group is not a free rotor, the three protons are no longer perfectly indistinguishable to the environment, but as a first order approximation, we treat them as identical spins.

One intuitive solution for accessing the $E_+/E-$ noiseless subsystem without breaking their degeneracy is to include a control Hamiltonian that selectively populates either the E_+ subsystem (logical $|\bar{0}\rangle$) or the E_- subsystem (logical $|\bar{1}\rangle$). We propose to first prepare Q_{LLS} with $\gamma \approx 1$, as it was explained in subsection 4.10.1. This step is done at very low temperature and very low field, which initializes the collective spin state in ρ_A that is polarized in terms of the spin symmetry label. In the next step, we apply a selective "π" pulse between $\Phi_{A,0}$ and $\Phi_{E_+,0}$ (or $\Phi_{E_-,0}$) on the torsional space. This leads to populating ρ_{E_-} (or ρ_{E_+} on the spin space without removing the degeneracy in the E subspace. We have not yet described how to implement these "π" pulses. This section is mostly devoted to exploring the possibility of addressing the logical basis (or $E_\pm$ subsystems) by using an interaction between the methyl group and a circularly polarized external electromagnetic field.

We are inspired by microwave spectroscopy [77, 85] which is a well known technique that uses the microwave irradiation to cause transitions between the rotational states of molecules in the gas phase. The emission and the absorption of the electric dipole allowed transitions leads to extracting information about the geometry of rigid bodies such as the bond's length and angles, [85, 86]. We adopt this technique and apply it to our case, where at low temperature the system is in the solid phase rather than the gas phase. At low field, we ignore the spin space and just focus on the spatial space transitions. Consider a rigid rotor in a $X-CH_3$ type molecule, whose torsional ground state splitting ΔE_0 is in the range of GHz. We explore whether a circularly (right or left) polarized microwave filed that is on resonance with ΔE_0, induces a transition between the $\Phi_{A,0}$ and the $\Phi_{E_\pm,0}$ or not.

A molecule with a permanent dipole moment $\vec{\mathbf{d}}$ interacts with a time varying electromagnetic field, $\vec{\mathbf{E}}(\mathbf{r},t)$, via an electric dipole Hamiltonian, $H_d = -\hbar\ \vec{\mathbf{d}}.\vec{\mathbf{E}}(\mathbf{r},t)$. For a point charge, the dipole moment is $\vec{\mathbf{d}}(\vec{\mathbf{r}}) = q\ \vec{\mathbf{r}}$, and for a charge distribution, the dipole moment is

$$\vec{\mathbf{d}}(\vec{\mathbf{r}}) = \int \rho_e(\vec{\mathbf{r}} - \vec{\mathbf{r}'})\ \vec{\mathbf{r}'}\ d^3\vec{\mathbf{r}'},$$

where $\rho_e(\vec{\mathbf{r}}) = |\psi_e(\vec{\mathbf{r}})|^2$ is the electron charge distribution. If the electromagnetic wavelength is much larger than the molecule size, the field is constant across the molecule, $\vec{\mathbf{E}}(\mathbf{r},t) \sim \vec{\mathbf{E}}(t)$. According to Fermi's Golden Rule, the probability of transition from the i^{th} level to the j^{th} level due to an interaction Hamiltonian $H_{\text{int}} = H_d$ is given by

$$\begin{aligned} W_{i\to j} &= \frac{2\pi}{\hbar}\ |\langle\psi_i|H_d|\psi_j\rangle|^2, \\ &= 2\pi\ \left(\int \psi_i^*(\vec{\mathbf{r}})\ \rho_e(\vec{\mathbf{r}})\ \vec{\mathbf{r}}.\vec{\mathbf{E}}(t)\ \psi_j(\vec{\mathbf{r}})d^3\vec{\mathbf{r}}\right)^2. \end{aligned} \tag{4.45}$$

The transition rate is proportional to an integral which is non-zero (allowed transitions) if and only if the integrand is a totally symmetric function, i.e., a transition from ψ_i to ψ_j is dipole allowed iff $\text{Sym}(\psi_i) \times \text{Sym}(H_{\text{d}}) \times \text{Sym}(\psi_j) = A$.

Excluding the spin space and the external rotations, $\psi_i(\vec{\mathbf{r}})$ is the internal rotation-vibration wave function. Based on the discussion in Section 4.6, at low temperature, the vibrational wavefunction is symmetric, and therefore, the symmetry of $\psi_i(\vec{\mathbf{r}})$ is determined by the symmetry of the torsional wavefunction, $\Phi_{\lambda,n}(\varphi)$. Moreover, the electron charge distribution $\rho_e(\vec{\mathbf{r}}) = |\psi_e(\vec{\mathbf{r}})|^2$, is also symmetric according to Section 4.5. Therefore, to find the selection rule (forbidden vs allowed transitions), it is sufficient to analyze the symmetry of $\Phi_{\lambda,n}\ \vec{\mathbf{r}}.\vec{\mathbf{E}}(t)\ \Phi_{\lambda',n'}$. Since we are only interested in the allowed transitions between $\Phi_{A,0}$ and $\Phi_{E_\pm,0}$, the only unknown component in the above integral, is the symmetry of $\vec{\mathbf{r}}.\vec{\mathbf{E}}(t)$.

A circularly polarized electromagnetic field is $\vec{\mathbf{E}}_\pm(t) = \mathscr{E}_0\ (\hat{x} \pm i\hat{y})\ e^{i\omega t}$ where $\mathscr{E}_0$ is the amplitude of the field [87]. Thus,

$$\vec{\mathbf{r}}.\vec{\mathbf{E}}_\pm(t) = \mathscr{E}_0\ (X \pm iY)\ e^{i\omega t} \tag{4.46}$$

According to the $\mathbf{C}_3$ group theory discussion in Section 4.3, one can find the symmetry of any spatial function by applying the symmetry projection operators to it. In particular, we apply $\hat{P}_A, \hat{P}_{E_+}$ and $\hat{P}_{E_-}$ on $(X+iY)$ and obtain

$$\begin{aligned} \hat{P}_A.(X+iY) &= 0, \\ \hat{P}_{E_+}.(X+iY) &= 0, \\ \hat{P}_{E_-}.(X+iY) &= (X+iY). \end{aligned} \tag{4.47}$$

This means that the electric dipole interaction with a *right circularly polarized* electromagnetic field has E_- symmetry. Therefore, for this particular interaction, the transition from $\Phi_{A,0}$ to $\Phi_{E_+,0}$ is symmetrically allowed. Similarly, a *left circularly polarized* field has the E_+ symmetry that results in the transition from $\Phi_{A,0}$ to $\Phi_{E_-,0}$. This is an interesting observation, because, it may enable us to selectively populate the E_+ or the E_- subspaces on the spin space resulting from the correlation between the torsional space and the spin space.

We introduce an effective Hamiltonian that takes into account both the electric dipole allowed transition due to the interaction with the right circularly polarized MW, and the spin-space correlation due to Pauli exclusion principle,

$$H_{\text{eff}} = \kappa \left(|\Phi_{E_-,0}\rangle\langle\Phi_{A,0}| \otimes \sum_{m\in\{\pm 1/2\}} |E_+,m\rangle\langle A,m| \right) + h.c.. \tag{4.48}$$

The strength of the coupling, κ, depends on the field amplitude $\mathscr{E}_0$ and the component of the electric dipole operator $\vec{\mathbf{d}}$ that is perpendicular to the symmetry axis. Before turning on the MW, and after the cooling, our system is initialized in[2]

$$\rho_0 = |\Phi_{A,0}\rangle\langle\Phi_{A,0}| \otimes \sum_{m=-3/2}^{3/2} \frac{1}{4} |A,m\rangle\langle A,m|. \tag{4.49}$$

Once we turn on a right circularly polarized MW for a time τ_0 so that $2\pi\kappa\tau_0 = \pi$, the collective spin system evolves to

$$\begin{aligned} \rho_{\text{spin}} &= Tr_{\text{tor}}\left[e^{-iH_{\text{eff}}\tau_0}\, \rho_0\, e^{+iH_{\text{eff}}\tau_0} \right] \\ &= \frac{1}{4}\left[\sum_{m\in\{\pm 3/2\}} |A,m\rangle\langle A,m| + \sum_{m\in\{\pm 1/2\}} |E_+,m\rangle\langle E_+,m| \right]. \end{aligned} \tag{4.50}$$

Therefore, the cooling followed by the MW irradiation effectively converts the population from $|A,\pm\frac{1}{2}\rangle$ to $|E_+,\pm\frac{1}{2}\rangle$ on the spin space. But, because of the mismatch of the dimension of the two subspaces, there is some undesired population left in the $|A,\pm\frac{3}{2}\rangle$ levels. Nevertheless, this is not an issue because of the scalar coupling between the methyl group and an external spin, such as carbon. This scalar coupling shifts the frequency of $m = \pm 1/2$ from that of $m = \pm 3/2$ and makes them distinguishable. Therefore, one can in principle post-select the E_+ events at the expense of decreasing the probability of success,

$$\rho_{\text{spin}}^{\text{post-select}} = \rho_{E_+} = \frac{1}{2} \sum_{m\in\{\pm 1/2\}} |E_+,m\rangle\langle E_+,m|. \tag{4.51}$$

[2]The spin eigenstates are simply denoted by $|s,m\rangle$ rather than $\psi_{s,m}$.

Similarly, the system is initialized in $\rho_{E_-} = \frac{1}{2} \sum_{m\in\{\pm 1/2\}} |E_-,m\rangle\langle E_-,m|$ via an interaction with the left circularly polarized MW. Thus, we have access to the logical basis states, $|\bar{0}\rangle = |E_+\rangle$ and $|\bar{1}\rangle = |E_-\rangle$, individually. By the right choice of the intensity of the left and right circularly polarized fields, one can create

$$Q_{\text{logic}} := \frac{(1+\beta)}{2}\rho_{E_+} + \frac{(1-\beta)}{2}\rho_{E_-}. \tag{4.52}$$

Q_{logic} is still a classical mixture of the logical states. To prepare any arbitrary superposition of the logical states, we require to implement an "X" gate which takes $|\bar{0}\rangle \leftrightarrow |\bar{1}\rangle$ and a "Z" which takes $|\bar{0}\rangle \rightarrow |\bar{0}\rangle$ and $|\bar{1}\rangle \rightarrow -|\bar{1}\rangle$. Given the logical gates, "X" and "Z", one has universal control over a single qubit [20]. We now show implementing these logical gates is feasible.

Suppose we are able to implement the following rotations:

$$\begin{aligned} U_\pm(\theta): \quad & |\Phi_{A,0}\rangle \otimes |A,m\rangle \\ \longrightarrow \quad & \cos\frac{\theta}{2}\,|\Phi_{A,0}\rangle \otimes |A,m\rangle + \sin\frac{\theta}{2}\,|\Phi_{E_\mp,0}\rangle \otimes |E_\pm,m\rangle, \end{aligned} \tag{4.53}$$

for $m = \pm\frac{1}{2}$. Given $U_\pm(\theta)$, the control gates are implemented by the following sequences:

$$\begin{aligned} X &:= U_-(\pi)\,U_+(\pi)\,U_-(\pi) \\ Z &:= U_-(2\pi)\,U_+(2\pi)\,U_-(2\pi) \end{aligned} \tag{4.54}$$

which act as

$$X: \quad \frac{1}{2}\left[|\Phi_{E_\mp,0}\rangle\langle\Phi_{E_\mp,0}| \otimes \sum_{m\in\{\pm 1/2\}} |E_\pm,m\rangle\langle E_\pm,m|\right] \tag{4.55}$$

$$\longrightarrow \quad \frac{1}{2}\left[|\Phi_{E_\pm,0}\rangle\langle\Phi_{E_\pm,0}| \otimes \sum_{m\in\{\pm 1/2\}} |E_\mp,m\rangle\langle E_\mp,m|\right] \tag{4.56}$$

$$Z: \quad \frac{1}{2}\left[|\Phi_{E_\mp,0}\rangle\langle\Phi_{E_\mp,0}| \otimes \sum_{m\in\{\pm 1/2\}} |E_\pm,m\rangle\langle E_\pm,m|\right]$$

$$\longrightarrow \pm \frac{1}{2}\left[|\Phi_{E_\mp,0}\rangle\langle\Phi_{E_\mp,0}| \otimes \sum_{m\in\{\pm 1/2\}} |E_\pm,m\rangle\langle E_\pm,m|\right]$$

Therefore, in principle, we have control over the logical subspace if we are able to implement an arbitrary rotation between the torsional eigenfunctions,$|\Phi_{A,0}\rangle \rightarrow \cos\frac{\theta}{2}|\Phi_{A,0}\rangle + \sin\frac{\theta}{2}|\Phi_{E_{\pm},0}\rangle$. This rotation can be achieved by controlling the intensity and the phase of the circularly polarized MW fields.

4.11 Observation via Relaxation

In the previous sections we explored how to initialize the collective spin state of a rigid rotor in Q_{LLS} by thermal means and/or Q_{logic} by MW irradiation. Both of these states are robust against collective noise. However, neither of them is observable in an NMR measurement. The reason is that if they are protected against collective noise, they are protected against the measurement as well. Quantitatively, $Tr[Q_{LLS}\,\hat{\mathbf{S}}_\alpha] = Tr[Q_{\text{logic}}\,\hat{\mathbf{S}}_\alpha] = 0$ for all $\alpha \in \{x,y,z\}$.

If there exists a quantum evolution process that does not preserve the cyclic permutation symmetry, it can in principle turn the symmetry polarization into the Zeeman polarization and hence make the protected state observable in NMR. One of the natural interactions that does not preserve the spin cyclic permutation symmetry is the dipolar interaction between spins which is the focus of our study. Another possibility is the CSA. In particular, this section studies the possibility of reading out a protected state by relying on relaxation processes induced by hetronuclear dipole-dipole interaction.

To initialize a protected state, we rely on cryogenic temperatures and low static field. But, in order to observe it, we propose to make a sudden jump in both temperature and magnetic field so that this time the torsional splitting can be neglected when compared to the Zeeman splitting. Moreover, at high temperature, the sample is not frozen any more and is in the liquid phase of the molecule, where all other types of molecular motions such as external rotation, translation and etc are expected. These extra degrees of freedom result in a randomly fluctuating dipolar interaction, which itself may result in observing the protected state.

For a $X-CH_3$ type molecule, there are two types of dipolar interactions that may affect the dynamics of the collective spin state: First, the homonuclear dipolar interaction within the methyl group. Due to indistinguishably of spins, this internal coupling preserves the spin cyclic permutation symmetry and therefore does not lead to observation of the protected states. Second, the hetronuclear dipolar interaction between the methyl group and an external spin I. That external spin could be from the same molecule (interamolecular interaction), or, it could be from some other molecule (intermolecular interaction). In the following, we first show that in general, the hetronuclear dipolar interaction does not preserve the spin cyclic permutation symmetry. Then, at high field, we apply the semi-classical Redfield relaxation theory and solve the master equation analytically in order to understand the underlying physics that eventually leads to observing

the protected states. This symmetry analysis of the dipolar interaction predicts some features of NMR peaks on both the proton channel and the external spin channel which is in agreement with experimental observation of LLS in methyl groups.

4.11.1 Symmetry of Dipolar Interaction in a Rigid Rotor

Two magnetic dipole moments $\vec{d}_1$ and $\vec{d}_2$ that are at a distance $\vec{\mathbf{r}}$ apart, interact through space via the *dipolar* Hamiltonian,

$$H_{\rm dip} = -\frac{\mu_0}{4\pi}\frac{1}{r^5}\left(3(\vec{d}_1.\vec{r})(\vec{d}_2.\vec{r}) - \vec{d}_1.\vec{d}_2\right). \tag{4.57}$$

Here, $\vec{d}_1 = \hbar\gamma_S\,\vec{S}$ and $\vec{d}_2 = \hbar\gamma_I\,\vec{I}$ with $\vec{S} = \frac{1}{2}\vec{\sigma}$ and $\vec{I} = \frac{1}{2}\vec{\sigma}$ for the case of spin half particles. The use of different symbols S and I emphasizes that these operators act on different Hilbert spaces and may represent two different spin species. The dipolar Hamiltonian is commonly written in a product form of spatial functions and rank-2 spin irreducible tensors,

$$\begin{aligned} H_{\rm dip} &= \sum_{q=-2}^{2} H_q \\ &= c_0 \sum_{q=-2}^{2} e^{-iq\varphi}\, F_q(r,\theta)\, \hat{T}_{2,q}, \end{aligned} \tag{4.58}$$

where $c_0 = -\frac{\hbar\mu_0\gamma_I\gamma_S}{4\pi}$ is a constant, $F_q(r,\theta)$ a function of space parameters and $\hat{T}_{2,q}$ a normalized bilinear spin operator. Explicitly,

$$\begin{aligned} \hat{T}_{2,0} &= \sqrt{\frac{2}{3}}\left(3S_zI_z - \vec{S}.\vec{I}\right), & F_0 &= \sqrt{\frac{3}{2}}\frac{1}{r^3}(3\cos^2\theta - 1), \\ \hat{T}_{2,\pm} &= \mp(S_zI_\pm + S_\pm I_z), & F_{\pm1} &= \mp\frac{3}{2}\frac{1}{r^3}\sin\theta\cos\theta, \\ \hat{T}_{2,\pm2} &= S_\pm I_\pm, & F_{\pm2} &= \frac{3}{4}\frac{1}{r^3}\sin^2\theta. \end{aligned} \tag{4.59}$$

Given these definitions, we have

$$\hat{T}^\dagger_{2,q} = (-1)^q\hat{T}_{2,-q}, \qquad Tr[\hat{T}^\dagger_{2,q}\hat{T}_{2,q'}] = \delta_{q,q'}, \qquad F_{-q} = (-1)^q F_q. \tag{4.60}$$

In case of homonuclear interaction, since $[S_z + I_z, \hat{T}_{2,q}] = q\,\hat{T}_{2,q}$, each $\hat{T}_q$ term changes the z component of the total spin magnetization from m to $m+q$. So, we may refer to q as the *order* number.

In the case of hetronuclear interactions, each $\hat{T}_{2,q}$ is further decomposed to $\hat{T}_{2,q} = \sum_p \hat{T}_{(q,p)}$ based on its commutation with the Zeeman Hamiltonian, i.e., $[\omega_s\ S_z + \omega_I\ I_z\ ,\ \hat{T}_{(q,p)}] = \omega_{(q,p)}\ \hat{T}_{(q,p)}$. The explicit form of these bilinear spin operators and their corresponding frequencies are listed in Table 4.7, but one can write them in a closed form by nothing $\hat{T}_{(q,p)} \propto S_p \otimes I_{q-p}$ and $\omega_{(q,p)} = p\omega_s + (q-p)\omega_I$, where I_0 or S_0 represents $\frac{\sigma_z}{2}$, and $I_\pm$ or $S_\pm$ represents $\frac{\sigma_x \pm i\sigma_y}{2}$.

q	$\hat{T}_{(q,p)}$			$\omega_{(q,p)}$		
	$p=1$	$p=0$	$p=-1$	$p=1$	$p=0$	$p=-1$
0	$-\frac{1}{\sqrt{6}}S_+I_-$	$\sqrt{\frac{8}{3}}S_zI_z$	$-\frac{1}{\sqrt{6}}S_-I_+$	$\omega_s - \omega_I$	0	$-\omega_s + \omega_I$
+1	S_+I_z	S_zI_+	—	ω_s	ω_I	—
+2	S_+I_+	—	—	$\omega_s + \omega_I$	—	—

Table 4.7: Components of the Dipolar Hamiltonian.

Given the above definitions, the hetronuclear coupling between the collective spins, $\mathbf{S}$, and the test spin, I, consists of three terms,

$$\begin{aligned} H_{\text{dip}}^{\mathbf{S}I} &= H_{\text{dip}}^{(1)} + H_{\text{dip}}^{(2)} + H_{\text{dip}}^{(3)} && (4.61) \\ &= c_0 \sum_{j=1}^{3} \sum_{q=-2}^{2} e^{-iq\varphi_j}\ F_q(r_j,\theta_j)\ \hat{T}_{2,q}^{j} \\ &= \sum_{q=-2}^{2} H_q^{\mathbf{S}I}, && (4.62) \end{aligned}$$

where $H_{\text{dip}}^{(j)}$ represents the dipole-dipole coupling between the j^{th} proton and the test spin and $\vec{\mathbf{r}}_j = (r_j, \theta_j, \varphi_j)$ is the relative distance between them in the Zeeman frame. Consider a particular geometry where the test spin I is located at the symmetry axis, and a particular molecular orientation where the symmetry axis is parallel to the field. Due to this special orientation, $r_j = r_0$ and $\theta_j = \theta_0$ or all $j \in \{1,2,3\}$ and $\varphi_1 = \varphi_0,\ \varphi_2 = \varphi_0 + \frac{2\pi}{3}$ and $\varphi_3 = \varphi_0 - \frac{2\pi}{3}$. Under the spin cyclic permutation, we obtain

$$\begin{aligned} F_q(r_j,\theta_j) &\rightarrow F_q(r_0,\theta_0) \quad \forall j \in \{1,2,3\}, && (4.63) \\ e^{-iq\varphi_1}\ \hat{T}_{2,q}^{1} + e^{-iq\varphi_2}\ \hat{T}_{2,q}^{2} + e^{-iq\varphi_3}\ \hat{T}_{2,q}^{3} &\rightarrow e^{-iq\varphi_1}\ \hat{T}_{2,q}^{2} + e^{-iq\varphi_2}\ \hat{T}_{2,q}^{3} + e^{-iq\varphi_3}\ \hat{T}_{2,q}^{1}. \end{aligned}$$

By replacing φ_j values, one concludes that each dipolar order picks up a different phase under the cyclic permutation. Indeed

$$P_+\ H_q^{\mathbf{S}I}\ P_+^T = e^{iq\frac{2\pi}{3}} H_q^{\mathbf{S}I}. \quad (4.64)$$

This implies that even in this particularly symmetrized orientation, the hetronuclear dipolar Hamiltonian does not preserve the spin cyclic permutation, i.e., $[P_+, \sum_q H_q^{\mathbf{SI}}] \neq 0$.

It is straightforward to extend this to any orientation of the molecule in space, and conclude that in general the hetronuclear dipolar Hamiltonian does not commute with the cyclic permutation transformation. Non commutativity of the dipoalr coupling with $\hat{P}_+$ implies that they do not have a common basis. Thus, a hetronuclear dipolar relaxation might lead to a process that takes the polarization from the symmetry order to the Zeeman order that is measurable.

4.11.2 Master Equation For Dipolar Relaxation

At high temperature and in liquid phase, the space coordinates $\vec{\mathbf{r}}_j(t) = (r_j, \theta_i, \varphi_i)$ randomly fluctuate in time, so does the dipolar Hamiltonian. In the absence of CSA, the total Hamiltonian consists of a Zeeman term $H_0 = \omega_h \hat{\mathbf{S}}_z + \omega_I \hat{I}_z$, a scalar coupling $H_{\text{scalar}} = 2\pi(J_0 \sum_{ij} \vec{S}^i.\vec{S}^j + J_1 \vec{\mathbf{S}}.\vec{I})$, and a fluctuating dipolar term $H_{\text{dip}}^{\mathbf{SI}}(t)$. The scalar coupling is totally symmetric and does not contribute to breaking the symmetry of the protected states, so, it is neglected in the following discussion, unless otherwise stated. At high field, we treat $H_{\text{dip}}^{\mathbf{SI}}(t)$ as a perturbation term and apply Redfield's semi-classical theory that was introduced in Section 2.4.1 to study the collective spin dynamics. In the following, we introduce the symmetrized irreducible rank-2 tensors and re-write the hetronuclear dipolar Hamiltonian in terms of them. These symmetrized operators provide insight about the key components of the dipolar coupling that leads into observing a protected state. Then, we solve the master equation analytically and anticipate the NMR signal.

We substitute $B_q^j = c_0 e^{-iq\varphi_j} F_q(r_j, \theta_j)$ in Equation 4.61 and re-write the dipoar Hamiltonian as [88, 89],

$$
\begin{aligned}
H_{\text{dip}}^{\mathbf{SI}}(t) = \sum_{q,p} & \quad \sum_{j=1}^{3} B_q^j(t)\, \hat{T}_{(q,p)}^j \\
= \sum_{q,p} \{ & + \frac{1}{3} \left(B_q^1 + B_q^2 + B_q^3\right) \left(\hat{T}_{(q,p)}^1 + \hat{T}_{(q,p)}^2 + \hat{T}_{(q,p)}^3\right) \\
& + \frac{1}{3} \left(B_q^1 + \varepsilon^* B_q^2 + \varepsilon B_q^3\right) \left(\hat{T}_{(q,p)}^1 + \varepsilon \hat{T}_{(q,p)}^2 + \varepsilon^* \hat{T}_{(q,p)}^3\right) \\
& + \frac{1}{3} \left(B_q^1 + \varepsilon B_q^2 + \varepsilon^* B_q^3\right) \left(\hat{T}_{(q,p)}^1 + \varepsilon^* \hat{T}_{(q,p)}^2 + \varepsilon \hat{T}_{(q,p)}^3\right) \} \\
= \sum_{q,p} & \quad \sum_{\lambda=0,\pm1} B_q^\lambda(t)\, \hat{T}_{(q,p)}^\lambda,
\end{aligned}
\tag{4.65}
$$

where $\varepsilon = e^{\frac{i2\pi}{3}}$. We emphasize that in the last line, the sum over different spins' indices is replaced by the sum over the symmetry label $\lambda \in \{0, \pm 1\}$ which corresponds to $\{A, E_\pm\}$ symmetries. The symmetrized complex functions B_q^λ and the symmetrized irreducible rank-2 tensors $\hat{T}^\lambda_{(q,p)}$ are given by

$$\begin{aligned} B_q^\lambda &:= \frac{1}{\sqrt{3}} \left(B_q^1 + \varepsilon^{\lambda *} B_q^2 + \varepsilon^\lambda B_q^3 \right), \\ \hat{T}^\lambda_{(q,p)} &:= \frac{1}{\sqrt{3}} \left(\hat{T}^1_{(q,p)} + \varepsilon^\lambda \hat{T}^2_{(q,p)} + \varepsilon^{\lambda *} \hat{T}^3_{(q,p)} \right). \end{aligned} \tag{4.66}$$

In a closed form, $\hat{T}^\lambda_{(q,p)} \propto \mathbf{S}_p^\lambda \otimes I_{q-p}$, where the bold notation reminds us that $\mathbf{S}_p^\lambda$ acts on all three spins. To clarify the effect of $\mathbf{S}_p^\lambda$ on the collective spin system, consider a simpler example of two spins, where $\varepsilon = e^{\frac{i2\pi}{2}} = -1$ and $\lambda \in \{0,1\}$ (or $\{A,E\}$). Thus, $\mathbf{S}_p^{A/E} \propto \left(S_p^1 \pm S_p^2 \right)$ is either symmetric or anti-symmetric. By looking at the non-zero matrix elements of $\mathbf{S}_p^\lambda$ in the triplet-singlet basis, we conclude that the symmetric tensors $\mathbf{S}_p^A$ causes transitions only *within* each symmetry subspace and the anti-symmetric tensors $\mathbf{S}_p^E$ causes transitions *between* two subspaces of the triplet states (A) and the singlet state (E). Indeed, for two spins we obtain

$$\mathbf{S}_p^\lambda = \frac{1}{\sqrt{2}} \left(S_p^1 + (-1)^\lambda S_p^2 \right) \; |j,m\rangle \longrightarrow |j+\lambda, m+p\rangle \tag{4.67}$$

where $j = 1$ is the triplet subspace and $j = 0$ is the singlet subspace.

Extending this to three spins is straightforward. Similarly, the $\mathbf{S}_p^A$ of three spins is a totally symmetric operator and it has non-zero matrix elements only within each symmetry subspaces A, E_+ or E_-. Consequently, it is block-diagonal in CPI basis. In a similar manner to the two-spin case, $\mathbf{S}_p^{E_\pm}$ links between two different symmetry subspaces. But, in case of three spins, $\mathbf{S}_p^{E_\pm}$ is neither symmetric nor anti-symmetric and one needs to be careful about the direction of transitions. We expand the $\mathbf{S}_p^{E_\pm}$ in the $|s,m\rangle$ basis and conclude that $\mathbf{S}_p^{E_+}$ transforms the symmetry of the eigenstates in *right cycle* as $(A \to E_+ \to E_- \to A)$ and the $\mathbf{S}_p^{E_-}$ transforms the symmetry of the eigenstates in *left cycle* as $(A \leftarrow E_+ \leftarrow E_- \leftarrow A)$. In summary, the upper index of $\mathbf{S}_p^\lambda$ determines whether the transformation is *within* each symmetry subspace ($\lambda = A$) or *between* them in a right/left cyclic direction ($\lambda = E_\pm$). And, the lower index determines the change in the the magnetization. Explicitly, when $p = 0$, $\mathbf{S}_0^\lambda$ takes $m \to m$ and when $p = \pm 1$ the $\mathbf{S}_\pm^\lambda$ takes $m \to m \pm 1$ for all values of λ. In other words,

$$\mathbf{S}_p^\lambda \; |s,m\rangle \longrightarrow |s+\lambda, m+p\rangle \tag{4.68}$$

where the sum in $s+\lambda$ is mod 3. The final remark is that the reverse process occurs via $(\mathbf{S}_p^\lambda)^\dagger$, where

$$(\mathbf{S}_p^\lambda)^\dagger = \mathbf{S}_{-p}^{-\lambda}. \tag{4.69}$$

For example, the transition from $|E_+, \frac{1}{2}\rangle$ to $|A, \frac{3}{2}\rangle$ occurs through $\mathbf{S}_+^{E_+}$ but the reverse process, from $|A, \frac{3}{2}\rangle$ to $|E_+, \frac{1}{2}\rangle$ occurs through $\mathbf{S}_-^{E_-}$. The allowed transitions due to $\mathbf{S}_+^\lambda$ are demonstrated in Figure 4.8. Now that we visualized the effect of these symmetrized irreducible tensors on the symmetrized eigenbasis, we proceed to solving the master equation.

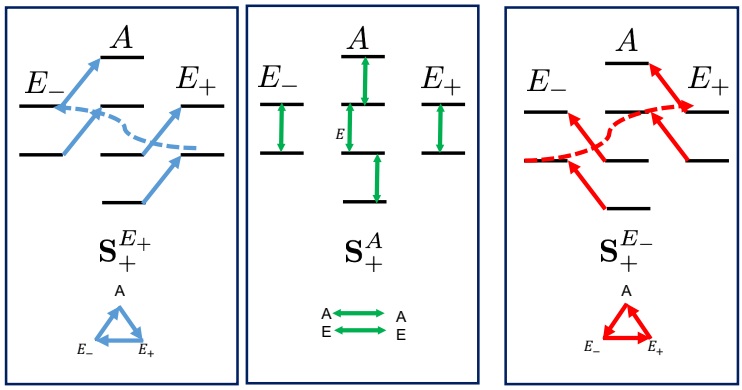

Figure 4.8: Allowed Transitions due to $\mathbf{S}_+^\lambda$: The non-zero transitions between the CPI states are demonstrated that are due to the non-zero matrix elements of the symmetrized collective spin operators $\mathbf{S}_+^\lambda$. The lower index $+$ acts on the magnetization label where it takes m to $m+1$ and the upper index λ acts on the symmetry label in a cyclic manner. The blue/red arrows indicate the non-zero transitions between different symmetry spaces in the right/left cyclic order and the green arrows refer to non-zero transition within each symmetry space.

Consider the Lindbladian form of the semi-classical master equation that was introduced in Section 2.4.1 and substitute $\hat{A}_\alpha$ operators with $\hat{T}^\lambda_{(q,p)}$

$$\frac{\partial\tilde{\rho}}{\partial t} = \sum_\lambda \sum_{q,p} J_q^\lambda(\omega_{(q,p)}) \hat{T}^\lambda_{(q,p)}\ \tilde{\rho}\ \hat{T}^{\lambda\dagger}_{(q,p)} - \frac{1}{2}\{\hat{T}^{\lambda\dagger}_{(q,p)}\hat{T}^\lambda_{(q,p)},\ \tilde{\rho}\}, \tag{4.70}$$

where $\tilde{\rho} = e^{iH_0t}\rho e^{-iH_0t}$ is the density matrix in the rotating frame of the Zeeman interaction. The coefficient $J_q^\lambda(\omega)$ is the real part of the symmetrized spectral density of noise and is defined by

$$\begin{aligned} J_q^\lambda(\omega) &:= \int_{-\infty}^{\infty} R_q^\lambda(\tau)\, e^{-i\omega\tau}\, d\tau, \\ R_q^\lambda(\tau) &:= \overline{B_q^\lambda(t)(B_q^\lambda)^*(t+\tau)}. \end{aligned} \tag{4.71}$$

Here, $R_q^\lambda(\tau)$ denotes the symmetrized auto correlation function and the overbar notation refers to averaging over the random variables. The imaginary part of the spectral density of noise leads into the dynamical shift and can be absorbed in the coherence evolution part [30].

For the purpose of the following discussion, the explicit form of the $J(\omega)$ is not required, because we are not interested in the exact dynamic of the system. Rather we would like to know which components of the hetronuclear dipolar coupling relax the collective spin system from Q_{LLS} or Q_{logic} into the measurable basis.

We define *Lindbladian map* with $\hat{D}[L][.] := \hat{L}\ .\ \hat{L}^\dagger - \frac{1}{2}\{\hat{L}^\dagger\hat{L},\ .\}$ in which L is the Lindblad operator and re-write the master equation as

$$\frac{\partial\tilde{\rho}}{\partial t} = \sum_\lambda \sum_{q,p} J_q^\lambda(\omega_{(q,p)})\ \eta_{q,p}\ \hat{D}[\mathbf{S}_p^\lambda \otimes I_{q-p}][\ \tilde{\rho}]. \tag{4.72}$$

where $\eta_{0.0} = 8/3$, $\eta_{0,\pm} = -1/6$ and $\eta_{q,p} = 1$ for all $q \neq 0$ cases. Considering classical noise $J_q^\lambda(\omega) = J_{-q}^{-\lambda}(-\omega)$ and neglecting $q = p = 0$ term which just shifts the energy, one can break the above master equation into three parts: the zero quantum transitions (ZQ), the double quantum transitions (DQ) and the single quantum transitions (SQ),

$$\begin{aligned}
\frac{\partial\tilde{\rho}}{\partial t} &= \sum_\lambda ZQ^\lambda[\tilde{\rho}] + DQ^\lambda[\tilde{\rho}] + SQ^\lambda[\tilde{\rho}] \qquad (4.73)\\
ZQ^\lambda[.] &:= \frac{1}{6} J_0^\lambda(\omega_s - \omega_I)\ \left(\hat{D}[\mathbf{S}_+^\lambda \otimes I_-][.] + \hat{D}[\mathbf{S}_-^{-\lambda} \otimes I_+][.]\right)\\
DQ^\lambda[.] &:= J_2^\lambda(\omega_s + \omega_I)\ \left(\hat{D}[\mathbf{S}_+^\lambda \otimes I_+][.] + \hat{D}[\mathbf{S}_-^{-\lambda} \otimes I_-][.]\right)\\
SQ^\lambda[.] &:= J_1^\lambda(\omega_s)\ \left(\hat{D}[\mathbf{S}_+^\lambda \otimes I_z][.] + \hat{D}[\mathbf{S}_-^{-\lambda} \otimes I_z][.]\right) + J_1^\lambda(\omega_I)\ \left(\hat{D}[\mathbf{S}_z^\lambda \otimes I_+][.] + \hat{D}[\mathbf{S}_z^{-\lambda} \otimes I_-][.]\right).
\end{aligned}$$

Here, we replace $(\mathbf{S}_p^\lambda)^\dagger = \mathbf{S}_{-p}^{-\lambda}$. The ZQ and the DQ terms exchange the energy between the collective spin and the test spin, and the SQ terms change either the collective spin states or the test spin states. As it was mentioned before, the totally symmetric Lindblad operators $\mathbf{S}_p^A \otimes I_{q-p}$ do not cause transition between two different symmetry subspaces of the collective spin. Therefore, if it happens that the spectral density of noise is very well approximated with just the totally symmetric component, i.e., $J_q^\lambda(\omega) \approx J_q^A(\omega)$, one can conclude that the system is very robust against noise and exhibits very long relaxation time. This is in agreement with the result in [84]. For the sake of simplicity in the following discussion, we ignore all the totally symmetric Lindblad operators, since they do not play a critical role in observing the protected state. We also neglect the $SQ^\lambda[.]$ terms, because we are interested in those transitions that the collective spin

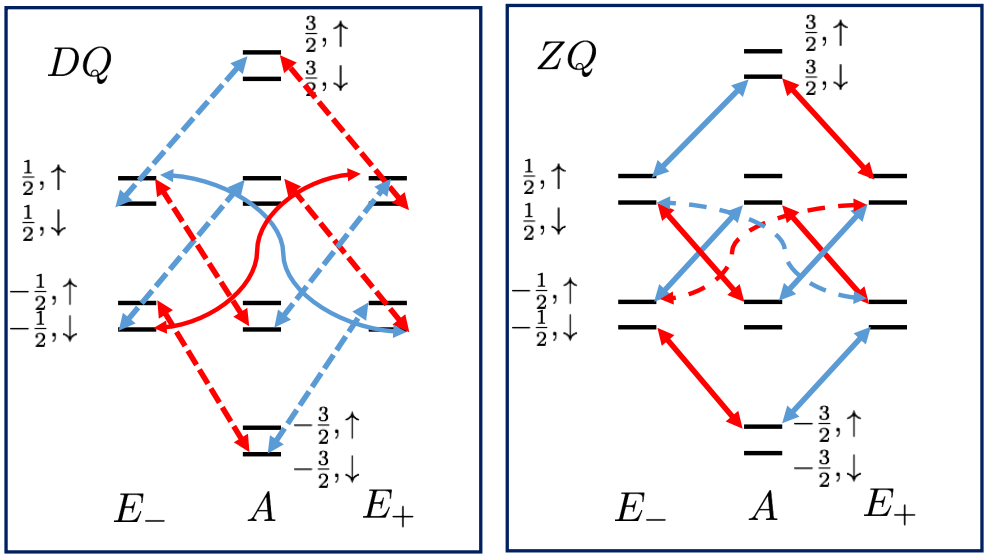

Figure 4.9: Left segment: The selection rule due to $DQ^{E_\pm}$ transitions. Right segment: The selection rule due to $ZQ^{E_\pm}$ transitions. Red vs blue refers to non-zero transitions due to $\mathbf{S}_p^{E_-}$ versus $\mathbf{S}_p^{E_+}$.

exchanges the energy with the test spin. The only important terms in the dissipator are $DQ^{E_\pm}$ and $ZQ^{E_\pm}$.

To obtain the allowed transitions due to ZQ and DQ terms, we need to calculate the effect of $\hat{D}[\mathbf{S}_p^\lambda \otimes I_\pm][.]$ on the eigenbasis $\{|s,m\rangle \otimes |\uparrow\rangle \text{or} |\downarrow\rangle\}$. The non-zero components are,

$$\begin{aligned}\hat{D}[\mathbf{S}_p^\lambda \otimes I_-][|s,m\rangle\langle s,m| \otimes |\uparrow\rangle\langle\uparrow|] = \quad & \mathbf{S}_p^\lambda\ |s,m\rangle\langle s,m|\ \mathbf{S}_p^\lambda)^\dagger \otimes I_-\ |\uparrow\rangle\langle\uparrow|\ I_+ \\ & -\frac{1}{2}\left(\mathbf{S}_{-p}^{-\lambda}\mathbf{S}_p^\lambda\ |s,m\rangle\langle s,m|\ \otimes I_+ I_-\ |\uparrow\rangle\langle\uparrow|\right) \\ & -\frac{1}{2}\left(|s,m\rangle\langle s,m|\ \mathbf{S}_{-p}^{-\lambda}\mathbf{S}_p^\lambda \otimes |\uparrow\rangle\langle\uparrow|\ I_+ I_-\right) \\ \propto \quad & |s+\lambda,m+p\rangle\langle s+\lambda,m+p| \otimes |\downarrow\rangle\langle\downarrow| - |s,m\rangle\langle s,m| \otimes |\uparrow\rangle\langle\uparrow|.\end{aligned} \tag{4.74}$$

Similarly,

$$\hat{D}[\mathbf{S}_p^\lambda \otimes I_+][|s,m\rangle\langle s,m| \otimes |\downarrow\rangle\langle\downarrow|] \propto |s+\lambda,m+p\rangle\langle s+\lambda,m+p| \otimes |\uparrow\rangle\langle\uparrow| - |s,m\rangle\langle s,m| \otimes |\downarrow\rangle\langle\downarrow|.$$

The proportionality constant is 1 for transitions from/to $m = \pm 3/2$ and is $\frac{1}{3}$ for all other levels.

Based on the above relations, the allowed transition due to $ZQ^{E_\pm}$ and $DQ^{E_\pm}$ terms are demonstrated in Figure 4.9 in which $\lambda = E_\pm$ transitions are color coded with red and blue respectively.

In general, the transition rates for the left rotation could be different from that of the right rotation and hence $J^{E_+}(\omega) \neq J^{E_-}(\omega)$, but if the noise is very symmetric in terms of the left/right rotation, we consider these two to be equal.

The calculation in Equation 4.74 convince us that if the initial state is a probabilistic mixture of different energy levels, the above master equation reduces to the classical rate equations,

$$\frac{d}{dt}p_x(t) = \sum_{y\neq x} W_{xy}\ \left(p_y(t) - p_x(t)\right), \tag{4.75}$$

where $p_x(t)$ is the population of the x^{th} energy level at time t with $x \in \{|s,m\rangle \otimes (|\uparrow\rangle \text{or} |\downarrow\rangle)\}$, and W_{xy} is the transition rate between two energy levels i and j. To solve the above differential equation, the evolution time is discretized into N steps where $t_N = N\delta t$ and δt is small compared to the energy scales of the system. Given the population distribution at time t_n, the change in the population of x^{th} level at time t_{n+1} is approximated by $\Delta p_x(n+1) \approx \delta t \times \sum_{xy} W_{xy}\ \left(p_y(n) - p_x(n)\right)$. Therefore, if the initial condition is known, one should be able to calculate the NMR signal by solving the rate equations recursively. Note that at any instance of time, $t = t_0 + \delta t$ the transition occurs only between those energy levels that first, are allowed due to $ZQ^{E_\pm}$ and $DQ^{E_\pm}$terms, and second, there is an imbalance of population at $t = t_0$.

The initial state of interest is

$$\rho_0 = \left(\begin{array}{c|c|c} \frac{1+\gamma}{2}\frac{\mathbb{1}}{4} & 0 & 0 \\ \hline 0 & \frac{1-\gamma}{2}\frac{1+\beta}{2}\frac{\mathbb{1}}{2} & 0 \\ \hline 0 & 0 & \frac{1-\gamma}{2}\frac{1-\beta}{2}\frac{\mathbb{1}}{2} \end{array}\right) \otimes \begin{pmatrix} \frac{1+\alpha}{2} & 0 \\ 0 & \frac{1-\alpha}{2} \end{pmatrix} \tag{4.76}$$

where γ is the amount of polarization between A symmetry subspace and E symmetry subspace, β is the amount of polarization between E_+ symmetry subsystem and E_- symmetry subsystem and α is the amount of polarization of the test spin. We chose this particular initial state because $\beta = 0$ corresponds to Q_{LLS} and $\gamma = -1$ corresponds to Q_{logic}. Since ρ_0 is diagonal, we alternatively represent it by a *population vector*

$$\vec{p}(0) = \begin{array}{c}\uparrow \\ \downarrow\end{array} \begin{pmatrix} \frac{1+\alpha}{2}\vec{q}_0 \\ \frac{1-\alpha}{2}\vec{q}_0 \end{pmatrix}, \qquad \text{where} \qquad \vec{q}_0 = \left(\begin{array}{c} \frac{(1+\gamma)}{2}\frac{1}{4}\begin{pmatrix}1\\1\\1\\1\end{pmatrix} \\ \hline \frac{(1-\gamma)}{2}\frac{(1+\beta)}{2}\frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \\ \hline \frac{(1-\gamma)}{2}\frac{(1-\beta)}{2}\frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} \end{array}\right) \begin{array}{c} A,\frac{3}{2} \\ A,\frac{1}{2} \\ A,-\frac{1}{2} \\ A,-\frac{3}{2} \\ E_+,\frac{1}{2} \\ E_+,-\frac{1}{2} \\ E_-,\frac{1}{2} \\ E_-,-\frac{1}{2} \end{array} \tag{4.77}$$

The $\vec{q}_0$ represents the vector of population of three identical spins at $t = 0$ in which all energy levels with the same symmetry label are equally populated, but, there is an imbalance of population between energy levels with different symmetry label. For use in future analysis, we compute those imbalance of populations and obtain

$$C_{\pm} := q_0^A - q_0^{E_{\pm}} = +\frac{\gamma}{4} \mp \beta \frac{(1-\gamma)}{8}, \tag{4.78}$$

$$C_2 := q_0^{E_+} - q_0^{E_-} = \beta \frac{(1-\gamma)}{4} = C_- - C_+, \tag{4.79}$$

where q_0^{λ} refers to the population of $|\lambda, m\rangle$ level for all possible values of m and at $t = 0$.

For the sake of abbreviation in notation, the population of the x^{th} energy level at time t, is denoted by $[x]_t$ instead of $p_x(t)$, and the change of population of the x^{th} level during the interval t_{n-1} and t_n, is denoted by $\Delta[x]_n$ instead of $\Delta p_x(n)$. Thus, $[x]_{t_n} = [x]_{t_{n-1}} + \Delta[x]_n$. Additionally, we denote $J_2^{\lambda}(\omega_s + \omega_I)$ with J_2^{λ} and $J_0^{\lambda}(\omega_s - \omega_I)$ with J_0^{λ}.

Considering an unpolarized test spin, $\alpha = 0$, the solutions to the rate equations for short

evolution time, $t = \delta t$, are

$$\begin{aligned}
\Delta[A,\tfrac{3}{2},\uparrow]_1 &= -\delta t\,\left(C_+\,J_2^{E_+} + C_-\,J_2^{E_-}\right), \\
\Delta[A,\tfrac{3}{2},\downarrow]_1 &= -\frac{1}{6}\delta t\,\left(C_+\,J_0^{E_+} + C_-\,J_0^{E_-}\right),
\end{aligned} \tag{4.80}$$

$$\begin{aligned}
\Delta[A,-\tfrac{3}{2},\uparrow]_1 &= -\frac{1}{6}\delta t\,\left(C_+\,J_0^{E_-} + C_-\,J_0^{E_+}\right), \\
\Delta[A,-\tfrac{3}{2},\downarrow]_1 &= -\delta t\,\left(C_+\,J_2^{E_-} + C_-\,J_2^{E_+}\right),
\end{aligned}$$

$$\begin{aligned}
\Delta[E_\pm,\tfrac{1}{2},\uparrow]_1 &= \delta t\,\left(\frac{1}{3}\left(C_\pm\,J_2^{E_\mp} \mp C_2\,J_2^{E_\pm}\right) + \frac{1}{6}C_\pm\,J_0^{E_\pm}\right), \\
\Delta[E_\pm,\tfrac{1}{2},\downarrow]_1 &= \delta t\,\left(\frac{1}{3\times 6}\left(C_\pm\,J_0^{E_\mp} \mp C_2\,J_0^{E_\pm}\right) + C_\pm\,J_2^{E_\pm}\right),
\end{aligned}$$

$$\begin{aligned}
\Delta[E_\pm,-\tfrac{1}{2},\uparrow]_1 &= \delta t\,\left(\frac{1}{3\times 6}\left(C_\pm\,J_0^{E_\pm} \mp C_2\,J_0^{E_\mp}\right) + C_\pm\,J_2^{E_\mp}\right), \\
\Delta[E_\pm,-\tfrac{1}{2},\downarrow]_1 &= \delta t\,\left(\frac{1}{3}\left(C_\pm\,J_2^{E_\pm} \mp C_2\,J_2^{E_\mp}\right) + \frac{1}{6}C_\pm\,J_0^{E_\mp}\right).
\end{aligned}$$

Because all energy levels in A subspace are equally populated at $t = 0$, in the absence of DQ^A and ZQ^A terms, we obtain $\Delta[A,\pm\frac{1}{2},\uparrow]_1 = \frac{1}{3}\Delta[A,\pm\frac{3}{2},\uparrow]_1$ and $\Delta[A,\pm\frac{1}{2},\downarrow]_1 = \frac{1}{3}\Delta[A,\pm\frac{3}{2},\downarrow]_1$. The expressions in Equation 4.80, may appear very complicated and it may sound difficult to get an insight about the relaxation. But, if we pay attention to the symmetry, there is a delicate and simple relation between the population of different energy levels. First of all, for all values of (s,m), the change in the population of $|s,m,\uparrow\rangle$ level is the same as that of $|s,m,\downarrow\rangle$ with just the difference of replacing $J_2^\lambda \leftrightarrow J_0^\lambda/6$. Second, the change of population in each level $|s,m,\uparrow\rangle$ is the same as that of $|s,-m,\uparrow\rangle$ with just the difference of replacing $J_2^\lambda \leftrightarrow J_0^{-\lambda}/6$. It will be shown that the anti-phase feature of the NMR peaks arises from these two properties which are also visually captured from Figure 4.9. For $m = \pm\frac{1}{2}$ subspace, after summing over the symmetry labels and

doing some algebra, we obtain

$$\begin{aligned}\sum_{\lambda}\Delta[\lambda,\pm\frac{1}{2},\uparrow]_1 &= -\Delta[A,\pm\frac{3}{2},\downarrow]_1,\\ \sum_{\lambda}\Delta[\lambda,\pm\frac{1}{2},\downarrow]_1 &= -\Delta[A,\pm\frac{3}{2},\uparrow]_1,\end{aligned} \tag{4.81}$$

where $\lambda \in \{A, E_{\pm}\}$. We see in the following that these very neat relations between different energy levels enable us to anticipate the NMR signal for any arbitrary spectral density of noise.

To be more specific, we start from the NMR signal on the test spin channel. The scalar coupling $J_1\ \vec{\mathbf{S}}.\vec{I}$ that was neglected so far, shifts the frequency of the test spin condition on the total spin magnetization of protons. Therefore, it is expected to observe 4 distinguishable peaks on the I channel corresponding to $m=\pm\frac{3}{2}$ and $m=\pm\frac{1}{2}$. We define a set of operators that projects the collective spins to these magnetization subspaces with

$$\begin{aligned}\Pi^{\pm\frac{3}{2}} &= |A,\pm\frac{3}{2}\rangle\langle A,\pm\frac{3}{2}|,\\ \Pi^{\pm\frac{1}{2}} &= \sum_{\lambda}|\lambda,\pm\frac{1}{2}\rangle\langle\lambda,\pm\frac{1}{2}|.\end{aligned} \tag{4.82}$$

For a short evolution time, the expected NMR peaks at the test spin channel are

$$\begin{aligned}\langle\Pi^{\pm\frac{3}{2}}\otimes I_z\rangle|_{\alpha=0}^{\delta t} &= \frac{1}{2}\left([A,\pm\frac{3}{2},\uparrow]_{\delta t}-[A,\pm\frac{3}{2},\downarrow]_{\delta t}\right)=\frac{\delta t}{8}\left[\pm\gamma\left(\Gamma^{E_-}+\Gamma^{E_+}\right)+\beta\frac{(1-\gamma)}{2}\left(\Gamma^{E_+}-\Gamma^{E_-}\right)\right],\\ \langle\Pi^{\pm\frac{1}{2}}\otimes I_z\rangle|_{\alpha=0}^{\delta t} &= \frac{1}{2}\left(\sum_{\lambda}[\lambda,\pm\frac{1}{2},\uparrow]_{\delta t}-[\lambda,\pm\frac{1}{2},\downarrow]_{\delta t}\right)=\langle\Pi^{\pm\frac{3}{2}}\otimes I_z\rangle|_{\alpha=0}^{\delta t},\end{aligned}$$

in which $\Gamma^{\lambda}:=J_2^{\lambda}-\frac{1}{6}J_0^{\lambda}$. To compute the above NMR signals, we used $[x]_{\delta t}=[x]_0+\Delta[x]_1$ and replaced the expressions from Equation 4.80 into it. Similarly, the anticipated NMR peaks on the proton channel are

$$\begin{aligned}\langle\mathbf{S}_z\otimes|\uparrow\rangle\langle\uparrow|\rangle|_{\alpha=0}^{\delta t} &= \frac{3}{2}\left([A,\frac{3}{2},\uparrow]_{\delta t}-[A,-\frac{3}{2},\uparrow]_{\delta t}\right)+\frac{1}{2}\sum_{\lambda}\left([\lambda,\frac{1}{2},\uparrow]_{\delta t}-[\lambda,-\frac{1}{2},\uparrow]_{\delta t}\right)\\ &= \frac{\delta t}{8}\left[\beta\frac{(1-\gamma)}{2}\left(\tilde{\Gamma}^{E_-}-\tilde{\Gamma}^{E_+}\right)+\gamma\left(\tilde{\Gamma}^{E_+}+\tilde{\Gamma}^{E_-}\right)\right]\\ &= -\langle\mathbf{S}_z\otimes|\downarrow\rangle\langle\downarrow|\rangle|_{\alpha=0}^{\delta t}\end{aligned} \tag{4.83}$$

in which $\tilde{\Gamma}^{\lambda}:=J_2^{\lambda}+\frac{1}{6}J_0^{\lambda}$.

There are two important remarks here: First, the 4 peaks on the test spin channel have an in-phase part and an anti-phase part which in general results in peaks with unequal amplitudes but the two peaks on the proton channel have the same amplitude and are anti-phase; second, If the left-rotation noise is identical to the right-rotation noise, we get $J^{E_+} = J^{E_-}$; consequently, the β dependent terms vanishes meaning that the polarization within the noiseless subsystem E is not observable.

It remains to solve the rate equations in case of $\alpha \neq 0$. When the test spin has some initial polarization, $\alpha \neq 0$,in Equation 4.78 additional terms show up. Precisely, the imbalance of population difference between different energy levels is now

$$\begin{aligned}
[A,m,\uparrow]_0 - [E_\pm,m',\downarrow]_0 &= C_\pm + \left(\frac{\alpha}{4} \pm \alpha\beta\frac{(1-\gamma)}{8}\right), \\
[A,m,\downarrow]_0 - [E_\pm,m',\uparrow]_0 &= C_\pm - \left(\frac{\alpha}{4} \pm \alpha\beta\frac{(1-\gamma)}{8}\right), \\
[E_+,m',\uparrow]_0 - [E_-,m',\downarrow]_0 &= C_2 + \alpha\frac{(1-\gamma)}{4}, \\
[E_+,m',\downarrow]_0 - [E_-,m',\uparrow]_0 &= C_2 - \alpha\frac{(1-\gamma)}{4},
\end{aligned} \tag{4.84}$$

$\forall m \in \{\pm\frac{3}{2},\pm\frac{1}{2}\}$ and $\forall m' \in \{\pm\frac{1}{2}\}$. By replacing these initial imbalance of population in the rate equation (Equation 4.75) and after doing some tedious calculations, we obtain

$$\begin{aligned}
\langle \Pi^{\pm\frac{3}{2}} \otimes I_z\rangle|^{\delta t}_{\alpha\neq 0} &= \langle \Pi^{\pm\frac{3}{2}} \otimes I_z\rangle|^{\delta t}_{\alpha=0} - \frac{\delta t}{8}\left[\alpha\ \left(\tilde{\Gamma}^{E_+} + \tilde{\Gamma}^{E_-}\right) \pm \alpha\beta\frac{(1-\gamma)}{2}\ \left(\tilde{\Gamma}^{E_+} - \tilde{\Gamma}^{E_-}\right)\right] \\
\langle \Pi^{\pm\frac{1}{2}} \otimes I_z\rangle|^{\delta t}_{\alpha\neq 0} &= \langle \Pi^{\pm\frac{1}{2}} \otimes I_z\rangle|^{\delta t}_{\alpha=0} - \frac{\delta t}{8}\left[\alpha\ \left(\tilde{\Gamma}^{E_+} + \tilde{\Gamma}^{E_-}\right) \pm \alpha\frac{(2\beta-1)}{3}\frac{(1-\gamma)}{2}\ \left(\tilde{\Gamma}^{E_+} - \tilde{\Gamma}^{E_-}\right)\right]
\end{aligned} \tag{4.85}$$

Interestingly, all terms that have β dependency are proportional to $J^{E_+}(\omega) - J^{E_-}(\omega)$. This means that the polarization within the noiseless subsystem is observable if the noise differentiates the methyl group's left-rotation from the right-rotation, which is intuitively true.

In case of $J^{E_+}(\omega) = J^{E_-}(\omega)$, Equation 4.85 reduces to

$$\begin{aligned}
\langle \Pi^{\pm\frac{3}{2}} \otimes I_z\rangle|^{\delta t}_{\alpha\neq 0} &= \frac{\delta t}{8}\left[\pm\gamma\ \left(\Gamma^{E_-} + \Gamma^{E_+}\right) - \alpha\ \left(\tilde{\Gamma}^{E_+} + \tilde{\Gamma}^{E_-}\right)\right] \\
\langle \Pi^{\pm\frac{1}{2}} \otimes I_z\rangle|^{\delta t}_{\alpha\neq 0} &= \frac{\delta t}{8}\left[\pm\gamma\ \left(\Gamma^{E_-} + \Gamma^{E_+}\right) - \alpha\ \left(\tilde{\Gamma}^{E_+} + \tilde{\Gamma}^{E_-}\right)\right]
\end{aligned} \tag{4.86}$$

The anti-phase contribution in the NMR peaks is proportional to the initial imbalance of population between the A symmetry subspace and the E symmetry subspace. The in-phase contribution is proportional to the polarization of the test spin that is dipole coupled with the three protons. Because we do not know the explicit value of different orders of the spectral density of noise, we cannot make any conclusion about the relative magnitude of these two contributions. Nevertheless, we can conclude that the peaks in pair of $(\frac{3}{2},\frac{1}{2})$ or $(-\frac{3}{2},-\frac{1}{2})$ have the same phase and the same amplitude. Now, if the noise differentiates the left-rotation noise from the right-rotation noise, $J^{E_+}(\omega) \neq J^{E_-}(\omega)$, even for the case of $\beta = 0$, we can no longer make any judgment about the relative amplitude and phase of these 4 peaks. Because, according to Equation 4.85, even when $\beta = 0$ an additional anti-phase term survives for the $m = \pm\frac{1}{2}$ peaks. In Chapter A, we compute the NMR peaks for one step further when $t = 2\delta t$ and conclude that for a longer evolution time, additional terms show up that diffrentiates the amplitude of the $m = \pm\frac{3}{2}$ from that of $m = \pm\frac{1}{2}$. Thus, 4 peaks with unequal amplitudes is expected. This argument holds for any arbitrary spectral density of noise and without any assumption about the magnitude of the anti-phase contribution relative to the in-phase contribution. Now, we assume those terms with a γ factor are larger than the others and conclude that the m peaks are overall anti-phase with the $-m$ peaks but with unequal amplitudes. A large γ corresponds to the long lived state that was experimentally demonstrated in [84], and surprisingly the above model, which considers only the $DQ^{E_\pm}$ and the $ZQ^{E_\pm}$ transitions of the DD coupling between the collective spin and an external spin, results in an analytic solution that predicts most features of the NMR peaks that have been experimentally observed.

4.12 Summary

In this chapter, we first reviewed the theoretical concepts developed in QIP which motivates the collective spin degree of freedom as a candidate for storing noise protected information. Next, we explored the possibility of experimental demonstration of the protected states in a methyl group. We analyzed the Hamiltonian and the eigenstructure of a methyl group and argued the symmetry of the wavefunction in terms of electron, vibration, internal rotation and spin. Furthermore, the symmetry restriction imposed by Pauli exclusion principle for fermions led to a symmetry correlation between the torsional space and the collective spin space. We used this correlation to propose an experiment that relies on MW irradiations and selection rules to initialize the collective spin in the noise protected subspace. We further analyzed the symmetry of DD coupling between the identical spins and a test external spin. We concluded that if the dipolar spectral density of noise is completely symmetric, i.e., $J^A(\omega)$, the protected states Q_{LLS} and/or Q_{logic} exhibit a very long relaxation time. Moreover, the pure non-symmetric parts of the

hetronuclear dipolar interaction, $DQ^{E_{\pm}}$ and $ZQ^{E_{\pm}}$ seems to be the the dominent component of the dipolar relaxation that leads to observing a noise protected state. The analytic calculation predicts four NMR peaks on the test spin channel with unequal amplitudes and anti-phaseing features which is in agreement with the experimental obsevations in [84].

Chapter 5

Quantum Key Distribution with Simplified Trusted Relay

5.1 Introduction

In the realm of cryptography, a secure communication is guaranteed if two legitimate users have access to a common secret key [90]. The task of *key distribution* protocols is to establish a secret key between two remote users (Alice and Bob) in the presence of an eavesdropper (Eve). The security of the classical key distribution protocols basically relies on the difficulty of solving a mathematical problem. In contrast, the security of the Quantum Key Distribution (QKD) protocols relies on the laws of quantum mechanics, where the more information Eve obtains, the more disturbance Alice and Bob detect in their data.

A common class of QKD protocols are known as *prepare and measure schemes*, which can be divided into two phases: the quantum phase and the classical phase. In the quantum phase, quantum states are distributed between legitimate users via a noisy quantum channel monitored by Eve. Afterwards, Alice and Bob measure their quantum states and each acquires a string of classical data. In the classical phase, Alice and Bob communicate through an authenticated classical channel and proceed with Parameter Estimation (PE), Error Correction (EC), and Privacy Amplification (PA) steps in order to first, have an estimate of how much information has leaked to Eve, and second, convert their raw data to a pair of *identical* and *secure* keys.

A significant challenge in practical QKD is to establish a secret key over any arbitrary distance. The maximum distance that is achieved in direct link QKD is restricted to 250 km by current technology [91]. One possible solution to increase the distance is to use a quantum network

with interconnections between legitimate users. In this setup, the intermediate nodes collaborate with the other users to finally establish a secret key between two disconnected, legitimate users.

An example of a quantum network in the existing experiments [13, 92] is a trusted relay (TR) network. For instance, a satellite as an intermediate node performs a complete QKD with each one of the two legitimate users on the ground, and establishes two independent secret keys: K_A and K_B. Afterwards, the satellite computes $K_A \oplus K_B$, and publicly announces the sum by which Alice's secret key is revealed to Bob. The announcement, $K_A \oplus K_B$, has no information about individual keys; thus, the protocol is secure. The negative aspect of this scheme is that the satellite gets involved in all steps of the quantum phase and the classical phase for each link, requiring significant computing and communication resources. In addition, at the end of the protocol, Alice and Bob plus the intermediate node have full access to the final secret key; thus, this node needs to be trusted.

Another example of a quantum network is a quantum repeater [14]. In link a, Alice possess one qubit of a maximally entangled state, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and sends the other part to an intermediate node; similarly, in link b, another entangled state is shared between Bob and the intermediate node. The middle node performs a joint measurement on the two independent signals (one from link a and one from link b) in Bell basis, correlating Alice's and Bob's data directly. In this way, the intermediate node takes part in the quantum phase only, and Alice and Bob carry out the classical phase. Additionally, the intermediate node has no information about the final secret key; thus, this node does not need to be trusted. Although the quantum repeater overcomes the concerns in the trusted relay network, it introduces experimental challenges. Performing the joint measurement requires a nearly perfect quantum memory, which is hard to implement. This situation has inspired us to consider a trade off between the quantum trusted relay and the quantum repeater: A protocol that reduces the intermediate node's involvement in the classical phase and removes the need for quantum memory.

In this chapter, we propose a simplified trusted relay (STR) protocol in which a new announcement made by the intermediate trusted nodes removes the need for substantial computing resources and communication. This protocol establishes a reasonable key rate between the two legitimate users in a quantum network and relieves the intermediate nodes from performing the Error Correction and the Privacy Amplification steps. They contribute only to the Parameter Estimation step. This new announcement strategy simplifies the task of intermediate nodes in the sense that, classically, there is no need for extensive amount of computing power, and quantumly, there is no need for quantum memory and joint measurements.

Section 5.2 provides some basic definitions in information theory. In Section 5.3 and Section 5.4, we review different steps of a conventional QKD protocol, and then in Section 5.5, we provide a framework for the security proof of prepare and measure schemes. Eventually, from

Section 5.7 to the rest of this chapter, we elaborate on our proposed STR protocol and examine its security.

5.2 Basic Definitions in Information Theory

5.2.1 Classical Information

1. **States:** In classical information theory, every event X is associated with a random variable with possible values $\{x_1, x_2, ...\}$. The statistical information about X is represented by a probability distribution $p(X)$. Correspondingly, to every classical information, $p(X)$, a classical density matrix, ρ_X, is assigned such that

$$\rho_X = \sum_X p(x)\ |x\rangle\langle x|. \tag{5.1}$$

   Here, for every classical value x a quantum state $|x\rangle\langle x|$ is associated.

2. **Uncertainty:** The so called *Shannon entropy* characterizes amount of *uncertainty* about an event X, and is defined by

$$H(X) = -\sum_X p(x)\log p(x) = -Tr[\rho_X \log \rho_X]. \tag{5.2}$$

3. **Composite System:** For two random variables, X and Y, with joint probability distribution $p(X,Y)$, the joint classical density matrix and the joint Shannon entropy are defined by

$$\begin{aligned} \rho_{XY} &= \sum_{X,Y} p(x,y)\ |x\rangle\langle x| \otimes |y\rangle\langle y|, \\ H(X,Y) &= -\sum_{X,Y} p(x,y)\ \log p(x,y) = -Tr[\rho_{XY}\log \rho_{XY}]. \end{aligned} \tag{5.3}$$

   For two correlated events X and Y, with $p(X,Y) \neq p(X)\ p(Y)$, the knowledge about event Y reduces the *uncertainty* about event X to

$$\begin{aligned} H(X|Y) &= H(X,Y) - H(Y), \\ &= -\sum_{X,Y} p(x,y)\log p(x|y), \end{aligned} \tag{5.4}$$

   which is known as *conditional Shannon entropy*. Here, the conditional probability distribution, $p(x|y) = p(x,y)/p(y)$, is given by *Bayes's rule*. The conditional Shannon entropy satisfies

$$H(X|Y) + H(Y) = H(Y|X) + H(X). \tag{5.5}$$

4. **Correlation:** The so called *mutual information* characterizes amount of *correlation* between two events, X and Y, and is defined by

$$I(X:Y) = H(X) - H(X|Y). \tag{5.6}$$

Intuitively, when we subtract the uncertainty about event X condition on knowing event Y from the total uncertainty about event X, we obtain amount of *common* information that is shared between the two events. When the two events are uncorrelated, we get $H(X|Y) = H(X)$; thus, the mutual information is simply zero.

5.2.2 Quantum Information

1. **States:** In quantum information theory, every event A is associated with a Hilbert space $\mathscr{H}_A$ and is referred as a *quantum register*. The statistical information about the quantum register A is represented by a quantum density matrix $\rho_A \in \Gamma(\mathscr{H}_A)$.

2. **Uncertainty:** Given ρ_A, the analogy to the Shannon entropy is the *von-Neumann entropy* that is defined by

$$S(A) \equiv S(\rho_A) = -Tr[\rho_A \log \rho_A]. \tag{5.7}$$

To compute this, we need to find a basis $\{|a_i\rangle\langle a_i|\}$ in which ρ_A is diagonal and has eigenvalues $\{a_i\}$. Then, $S(\rho_A) = -\sum_i a_i \log a_i$.

3. **Composite System:** Similar to the classical case, for a composite system AB with *joint* density matrix $\rho_{AB} \in \Gamma(\mathscr{H}_A \otimes \mathscr{H}_B)$, the von-Neumann entropy is defined by

$$S(A,B) \equiv S(\rho_{AB}) = -Tr[\rho_{AB} \log \rho_{AB}]. \tag{5.8}$$

Often in QKD we deal with a composite system where one party has classical information and the other party has quantum information. In that case, the classical-quantum (cq) density matrix is defined by

$$\rho_{XB} = \sum p(x)|x\rangle\langle x| \otimes \rho_B^x, \tag{5.9}$$

where for every classical information x held by the first party, the second user has a *conditional* quantum density matrix, ρ_B^x. Given ρ_{XB}, the classical-quantum von-Neumann entropy is given by

$$\begin{aligned} S(X,B) \equiv S(\rho_{XB}) &= -Tr[\rho_{XB} \log \rho_{XB}] \\ &= H(X) + \sum_X p(x)\, S(\rho_B^x). \end{aligned} \tag{5.10}$$

The last term in the above equation is known as cq-conditional von-Neumann entropy

$$S(B|X) = \sum_X p(x)\, S(\rho_B^x). \tag{5.11}$$

$S(B|X)$ measures amount of uncertainty about a quantum event B provided that the classical information X, is known.

4. **Correlation:** The notion of the *Holevo quantity* is introduced to quantify the amount of *correlation* between a classical register and a quantum register

$$\begin{aligned} \chi(X:B) &\equiv \chi(\rho_{XB}) = H(X) - S(X|B). \\ &= S(B) - S(B|X) \end{aligned} \tag{5.12}$$

In summary, in classical (quantum) information theory, for given statistical information $p(X,Y)$ or ρ_{AB} about two events (register), (X,Y) or (A,B), the uncertainty about individual events is quantified by Shannon (von-Neumann) entropy and the amount of correlated information between two events is quantified by mutual information (Holevo quantity).

We close this section by two theorems that are often used in quantum information theory.

Theorem 5.1. ***(Schmidt Decomposition):*** *Given a pure state $|\Psi\rangle_{AB} \in \mathscr{H}_{AB}$, there exist an orthonormal basis $\{|i_A\rangle\} \in \mathscr{H}_A$ and $\{|i_B\rangle\} \in \mathscr{H}_B$ such that*

$$|\Psi\rangle_{AB} = \sum_i \sqrt{p_i}\, |i_A\rangle \otimes |i_B\rangle, \tag{5.13}$$

where $p_i \geq 0$ and $\sum_i p_i = 1$. The basis $|i_A\rangle$ and $|i_B\rangle$ are called Schmidt basis and $\{\sqrt{p_i}\}$ are Schmidt coefficients.

A useful consequence of the Schmidt decompotion is that if a joint quantum state, ρ_{AB}, is a pure state, one can show $S(\rho_A) = S(\rho_B)$ [20].

Theorem 5.2. ***(Purification):*** *Given a mixed state $\rho_A = \sum_i p_i\, |\psi_i\rangle\langle\psi_i|$ there exist a pure state, $|\Psi\rangle_{AB} \in \mathscr{H}_{AB}$, in a larger Hilbert space, so that $\rho_A = Tr_B[|\Psi\rangle\langle\Psi|_{AB}]$. The composite state $|\Psi\rangle_{AB}$ is called a purification of ρ_A with the Schmidt decomposition*

$$|\Psi\rangle_{AB} = \sum_i \sqrt{p_i}\, |\psi_i\rangle_A \otimes |i\rangle_B. \tag{5.14}$$

Note that the purification of ρ_A is unique up to an arbitrary unitary acting on B. Indeed, any state $|\Psi\rangle_u = (\mathbb{1} \otimes U)|\Psi\rangle$ is also a purification of ρ_A.

5.3 Quantum Phase of QKD

5.3.1 Quantum Signal Resources

In the quantum phase of the *prepare and measure* QKD schemes, Alice chooses a quantum state $|\phi_x\rangle$ with probability $p(x)$ from a set of quantum signal resources, $S = \{|\phi_{x_1}\rangle, |\phi_{x_2}\rangle, ...\}$, and sends the quantum signal to Bob through a noisy quantum channel (monitored by Eve). She repeats this process n times, where n is normally a very large number and asymptotically $n \to \infty$. This is the *preparation* step. In general, each $|\phi_x\rangle \in \mathscr{H}_d$ is a d-dimensional quantum state prepared in a quantum basis $u \in \mathfrak{B}(\mathscr{H}_d)$, where $\mathfrak{B}(\mathscr{H})$ denotes the set of all possible bases on Hilbert space $\mathscr{H}$. Thus, the label x is a string that contains both *bit information* and *basis information*. For example, in the well-known BB84 protocol, which was introduced by Bennett and Brassard in 1984, the signal resource is $S = \{|\uparrow\rangle, |\downarrow\rangle, |+\rangle, |-\rangle\}$ where $\{|\uparrow\rangle, |\downarrow\rangle\}$ are eigenvectors of σ_z and $\{|+\rangle, |-\rangle\}$ are eigenvectors of σ_x. Each of these bases represents a logical basis $\{|0\rangle, |1\rangle\}$. In this example, $x = (d,u)$ where $d \in \{0,1\}$ and $u \in \{X,Z\}$. The logical basis $\{|0\rangle, |1\rangle\}$ is also referred to as the *computational* basis or the *canonical* basis.

One can treat the preparation step in an alternative approach known as *source replacement* scheme. In a hypothetical experiment, we assume Alice prepares an entangled state

$$|\Phi\rangle_{AA'} = \sum_X \sqrt{p(x)}\ |x\rangle_A \otimes |\phi_x\rangle_{A'}, \tag{5.15}$$

keeps the quantum register A for herself and sends the other register A' to Bob. Once Bob receives his other half, Alice performs a POVM measurement $\mathbf{M}_A = \{\mathscr{A}_x\}$ with $\mathscr{A}_x = |x\rangle\langle x|$ on her part. Alice's measurement collapses Bob's state to $|\phi_x\rangle$. The prepare and measurement scheme and the source replacement scheme are theoretically equivalent, but the later one is more convenient in analysing the security proof of the QKD schemes. Therefore, for the rest of this chapter, we consider the source replacement scheme for describing the quantum signal resources of the QKD protocols.

5.3.2 Noise on Quantum Channel

In quantum phase, Alice communicates with Bob through a noisy quantum channel monitored by Eve. As a result, the flying pure state $|\phi_x\rangle$ transforms to a noisy quantum state ρ_B^x when arrives at Bob's laboratory. Indeed, Bob's quantum information is given by a mixed state ρ_B^x due to the correlation with the eavesdropper. For the security proof of the QKD protocols there are several assumptions made which are often in Eve's favour:

1. Eve has access to unlimited quantum resources and she can implement any types of unitary operator as long as it is permitted by the laws of quantum mechanics. For example, she cannot duplicate a quantum state according to the *no-cloning* theorem.

2. Eve does not have physical access to Alice's and Bob's laboratories but she knows how their equipment is performing. This means Eve can never alter Alice's state, which is the reference signal.

3. Eve can have quantum interference with Alice and Bob's communication but she cannot intervene on the classical communication. This means Alice and Bob communicate over an authenticated classical channel which does not allow Eve to alter their messages and she just listens to their conversations.

We assume any noise over the quantum communication channel is due to Eve's interference and name it as *Eve's attack*. In Eve's attack, she disturbs Alice and Bob's quantum communication by attaching an ancillary register $|E'\rangle$ to the flying information $|\phi_x\rangle_{A'}$ and performing a unitary operator on the composite system, $A'E'$. Since Eve's interaction is a unitary, the purity of the combined three quantum registers does not change. Thus,

$$\begin{aligned} |\Psi\rangle_{ABE} &= (\mathbb{1}_A \otimes U_{A'E'\to BE})(|\Phi\rangle_{AA'} \otimes |E'\rangle) \\ &= \sum_X \sqrt{p(x)}\ |x\rangle \otimes |\psi^x\rangle_{BE}, \end{aligned} \tag{5.16}$$

in which $|\psi^x\rangle_{BE} = U(|\phi_x\rangle_{A'} \otimes |E'\rangle)$ is also a pure state. Alternatively, one can apply the system-environment representation and describe Eve's attack by a CPTP map

$$\mathscr{E}[\rho] = Tr_E[U(\rho \otimes |E'\rangle\langle E'|)U^\dagger].$$

In fact, the CPTP map $\mathscr{E}$ represents the quantum noise over the quantum communication channel which transforms the density matrix of Alice and Bob as

$$\begin{aligned} \rho_{AB} &= (\mathbb{1} \otimes \mathscr{E}_{A'\to B})[(|\Phi\rangle\langle\Phi|_{AA'})] \\ &= \sum_X p(x)\ |x\rangle\langle x| \otimes \rho_B^x \end{aligned} \tag{5.17}$$

in which $\rho_B^x = \mathscr{E}[(|\phi_x\rangle\langle\phi_x|]$ is the noisy quantum state received by Bob. $|\Psi\rangle_{ABE}$ in Equation 5.16 is a purification of ρ_{AB} in Equation 5.18 with $\dim(\mathscr{H}_E) = \dim(\mathscr{H}_A \otimes \mathscr{H}_B)$, where $\dim(\mathscr{H})$ denotes the dimension of the Hilbert space. There is a constraint of $\rho_A = Tr_B[\rho_{AB}] = Tr_{A'}[|\Phi\rangle\langle\Phi|_{AA'}]$, because Eve does not have access to Alice's laboratories, her state is the same before and after the attack. It is important to note that the reduced density matrix $\rho_{AB} = Tr_E[|\Psi\rangle\langle\Psi|_{ABE}]$

is not a pure state, because Bob's quantum states is now correlated with a third party. According to the Choi-Jamiolkowski isomorphism given in Equation 2.58, characterising the noise over quantum communication channel, $\mathscr{E}$, is equivalent to characterizing the noisy joint quantum states ρ_{AB}.

What we described so far is one kind of Eve's quantum attack where Eve applies an identical unitary on each signal to correlate her register $|E'\rangle$ with the flying quantum state. After that, she either makes a measurement right away or she waits until the end of the protocol and applies a collective measurement on all n registers at once. The former is known as the *individual* attack and the latter is known as the *collective* attack. For the purpose of this thesis we restrict our discussion to the collective attacks. In both cases, the joint quantum state of all n signals is written as $\rho_{AB}^{n} = \rho_{AB}^{\otimes n}$, because Eve's attack in each round is independent of the other.

There is also a more general class of attacks called *coherent attack* where Eve collects all flying signals $A'^{\otimes n}$ and correlates them with a large register E' by applying a very large unitary on them. In this case, $\rho_{AB}^{n} \neq \rho_{AB}^{\otimes n}$ and the security proof is more complicated and is beyond the scope of this thesis.

5.3.3 Measurements

Once the quantum signals are distributed, the legitimate users perform their local measurements with POVMs $\mathbf{M}_A = \{\mathscr{A}_x\}$ and $\mathbf{M}_B = \{\mathscr{B}_y\}$, and obtain strings of classical information, $X = \{x_1, x_2, x_3, ..., x_n\}$ and $Y = \{y_1, y_2, ..., y_n\}$, respectively. The joint information of Alice, Bob and Eve is described by a classical-classical-quantum (ccq) density matrix, given by

$$\rho_{XYE} = \sum_{X,Y} p(x,y)\ |xy\rangle\langle xy|_{AB} \otimes \rho_E^{xy}, \tag{5.18}$$

where $p(x,y)$ is the joint statistical information about Alice and Bob's data and ρ_E^{xy} is Eve's conditional quantum state. Precisely,

$$\begin{aligned} p(x,y) &= Tr[(\mathscr{A}_x \otimes \mathscr{B}_y)\ \rho_{AB}], \\ \rho_E^{xy} &= Tr_{AB}[(\mathscr{A}_x \otimes \mathscr{B}_y \otimes \mathbb{1})\ |\Psi\rangle\langle\Psi|_{ABE}]/p(x,y). \end{aligned} \tag{5.19}$$

For further analysis, it is useful to introduce a few notations. First, Alice and Bob's measurement is represented by a joint POVM operator, $\mathbf{M}_{AB} = \mathbf{M}_A \otimes \mathbf{M}_B$, and second, the ccq-density matrix ρ_{XYE} is equivalently represented by $\rho_{XYE} \equiv \{|\Psi\rangle_{ABE}, \mathbf{M}_{AB}\}$. The latter notation emphasizes that the classical information is extracted from a quantum state by performing a quantum measurement on it, and this notation is borrowed from references [93] and [94].

After the measurement step, Alice knows her own statistics, $p(x) = Tr[(\mathscr{A}_x \otimes \mathbb{1})|\Phi\rangle\langle\Phi|_{AA'}]$, and Bob knows his own conditional probability distribution

$$p(y|x) = Tr[\mathscr{B}_y\ \rho_B^x]. \tag{5.20}$$

However, neither Alice nor Bob knows the joint probability distribution, $p(x,y)$. Thus, Alice and Bob communicate over an authenticated classical channel to estimate their joint information, $p(x,y) = p(x)\ p(x|y)$.

5.4 Classical Phase of QKD

By the end of the quantum phase, Alice has sent n signals, Alice and Bob have performed their local measurements, $\mathbf{M}_{AB}$, and two strings of raw data, $X = \{x_1, x_2, x_3, ..., x_n\}$ and $Y = \{y_1, y_2, ..., y_n\}$, have been obtained. The first task of the classical phase is to quantify the amount of mutual information between X and Y, and to estimate an upper bound on the amount of information that is leaked to Eve. If the estimated *leakage* of information is below a certain threshold, Alice and Bob proceed with a classical error correction and privacy amplification in order to map their raw data to a pair of *secure* and *identical* key string. An explicit description of these data processing steps is as the following:

1. *Parameter Estimation (PE):* Alice and Bob *sacrifice* n_{PE} bits of their information in order to *characterize* their joint statistical information, $p(X,Y) \equiv \rho_{XY}$. Given $p(X,Y)$ Alice and Bob are able to *estimate* an upper bound on the amount of information that is leaked to Eve during the quantum phase. If they conclude Eve is *highly* correlated with their data, they abort the protocol. Otherwise, they proceed to the next step.

2. *Announcement and Post Selection:* In some QKD schemes, Alice and Bob make an announcement and use it for further data processing. For example, given the announcement, the users may decide to *keep* their data or *ignore* it or they may apply certain operations on their raw data to enhance their mutual correlation.

3. *Error Correction (EC):* If the error estimated in the parameter estimation step is below a certain threshold, the protocol is not aborted, and Alice and Bob run the error correcting algorithms to enhance the correlation between their data. $H(X|Y)$ quantifies the amount of error correction that is required. If $H(X|Y) > H(X)$, the protocol is aborted because Alice and Bob's mutual information is not positive. If it is positive, they proceed to the next step.

4. *Privacy Amplification* If the QKD protocol is not aborted in the PE and the EC steps, Alice and Bob use the well-known classical algorithms to map their raw data to shorter, *identical* and *secure* key strings. The users shorten the data so that any possible information that may have leaked to Eve during the quantum phase, as well as other classical communication steps, is removed.

The above steps are not in chronological order, and depending on the protocol, their orders may differ or they might be done in parallel.

5.5 Security Proof Formalism

5.5.1 Security Definition

If the QKD protocol succeeds, the two users' individual raw data, X and Y each with length n, is mapped to identical strings, $k_A = k$ and $k_B = k$, each with a shorter length l. Every key string k is associated with a classical density matrix $\rho_K \in \mathscr{H}_k$, and correspondingly, Eve's knowledge about the secret key is associated with a quantum state $\rho_{E_k} \in \mathscr{H}_{E_k}$. The classical-quantum composite state of the key and Eve is denoted by $\rho_{KE_k} \in \mathscr{H}_k \otimes \mathscr{H}_{E_k}$. Intuitively, if Eve's state is uncorrelated from the key, ρ_{KE_k} is not only a separable state but is also a product state. Formally, the key string, k, is defined to be ε-*secure* if

$$\frac{1}{2}|\rho_{KE_k} - \mathbb{1}_K \otimes \rho_{E_k}|_1 \leq \varepsilon, \tag{5.21}$$

where $|.|_1$ is the trace norm. In the ideal case, when k is a totally random string, we have $\rho_k = \mathbb{1}_K$, which is a perfect key to comprise future cryptography algorithms.

5.5.2 Key Rate

By the end of a successful QKD protocol, n quantum signals are distributed, out of which two secure and identical keys, each with length l, are generated. The rate at which Alice and Bob establish the secret key quantifies the efficiency of the QKD protocol. In the asymptotic limit, the key rate is

$$R_\infty = \lim_{n\to\infty} \frac{l}{n}. \tag{5.22}$$

In this limit, the mutual information, $I(X:Y)$, measures the number of error-free bits that are shared between the legitimate users, and the Holevo quantity, $\chi(X:E)$, measures the number of

bits that have leaked to the third party. Therefore, the key rate is practically computed by [95]

$$R_\infty = I(X:Y) - \chi(X:E). \tag{5.23}$$

In quantum information theory, the lower bound of the key rate is of interest, because it corresponds to the worst-case scenario. This lower bound is computed as a function of the error rate, which indicates how much noise is tolerable by the QKD protocol in order to establish a secret key at a positive rate.

The first term of the key rate, $I(X:Y)$, is computed in the Parameter Estimation step when Alice and Bob characterize the joint probability distribution, $p(x,y)$ by which the amount of correlation between their data is computed using the definition in Equation 5.6.

The computation of the second term of the key rate, $\chi(X:E)$, is a little bit tricky. Given the definitions in Equation 5.24 and Equation 5.11, the amount of correlation between Alice's classical information and Eve's quantum knowledge is quantified as

$$\begin{aligned} \chi(X:E) = \chi(\rho_{XE}) &= S(\rho_E) - \sum_X p(x)\, S(\rho_E^x) \\ &= S(\rho_{AB}) - \sum_X p(x)\, S(\rho_B^x). \end{aligned} \tag{5.24}$$

In last line, $S(\rho_E) = S(\rho_{AB})$ and $S(\rho_E^x) = S(\rho_B^x)$ due to the fact that $|\Psi\rangle_{ABE}$ and $|\psi^x\rangle_{BE}$ are pure states according to Equation 5.16. The above relation states that if Alice and Bob have a good estimation of their joint quantum state, ρ_{AB}, they are able to estimate the amount of *leakage* to Eve. However, after the *PE* step, what Alice and Bob have access to is not the quantum state ρ_{AB}, but rather the classical state ρ_{XY}. In fact, the statistical information $p(x,y)$, or equivalently the cc-density matrix ρ_{XY} and the local measurement $\mathbf{M}_{AB}$ do not uniquely determine the quantum state ρ_{AB}. Thus, to be on the safe side, among all possible states ρ_{AB} that are compatible with Alice's and Bob's statistics, (i.e., satisfy $\rho_{XY} \equiv \{\rho_{AB}, \mathbf{M}_{AB}\}$), we consider the one that maximizes Eve's information.

Definition 5.3. The subset $\Gamma_{XY} \subset \Gamma(\mathscr{H}_{AB})$ is a set of all density matrices that are compatible with the statistical information $p(X,Y)$ due to the local measurements $\mathbf{M}_{AB} = \{\mathscr{A}_x \otimes \mathscr{B}_y\}$ such that

$$\Gamma_{XY} = \{\rho_{AB} \in \Gamma(\mathscr{H}_{AB}) \mid p(x,y) = Tr[(\mathscr{A}_x \otimes \mathscr{B}_y)\, \rho_{AB}]\}. \tag{5.25}$$

Given the above definition, the upper bound on Eve's knowledge is quantified by

$$\chi(X:E) = \chi(\{\rho_{AB}, \mathbf{M}_{AB}\}) \leq \max_{\rho \in \Gamma_{XY}} \{S(\rho_{AB}) - \sum_X p(x)\, S(\rho_B^x)\}. \tag{5.26}$$

Therefore, computing the *lower bound* on key rate requires an optimization over the set Γ_{XY} under the constraint that Alice's state is intact, i.e., $\rho_A = Tr_B[\rho_{AB}] = Tr_{A'}[|\Phi\rangle\langle\Phi|_{AA'}$. Thus,

$$R \geq \inf_{\rho \in \Gamma_{XY}} (I(X:Y) - \chi(\{\rho_{AB}, \mathbf{M}_{AB}\}). \tag{5.27}$$

5.5.3 Announcement

In some QKD schemes, Alice and Bob make some announcements to maximize the correlation between their data and/or to facilitate their data processing. For example, in BB84 protocol, the legitimate users announce their basis of measurement and if their basis matches, they keep the corresponding bit information; Otherwise, they ignore it. In the following, we provide a mathematical description of the announcement step that fits into the security proof formalism.

Suppose that for each pair of data, (x,y), Alice and Bob announce $\vec{u} = (f_A(x), f_B(y))$ with probability $p(\vec{u})$. Based on the announcement $\vec{u} = (u_1, u_2)$, the set of all data is repartitioned into a sum of subsets, $X = \cup X_{u_1}$ and $Y = \cup Y_{u_2}$, where $X_{u_1} = \{x \in X | f_A(x) = u_1\}$ and $Y_{u_2} = \{y \in Y | f_B(y) = u_2\}$. Correspondingly, the set of measurement operators is repartitioned into subsets, $\mathbf{M}_A = \cup \tilde{\mathbf{M}}_A^{u_1}$ and $\mathbf{M}_B = \cup \tilde{\mathbf{M}}_B^{u_2}$, where

$$\begin{aligned} \tilde{\mathbf{M}}_A^{u_1} &= \{\tilde{\mathbf{A}}_x^{u_1} := \mathscr{A}_x | x \in X_{u_1}\}, \\ \tilde{\mathbf{M}}_B^{u_2} &= \{\tilde{\mathbf{B}}_y^{u_2} := \mathscr{B}_y | y \in Y_{u_2}\}, \end{aligned} \tag{5.28}$$

and $\tilde{\mathbf{M}}_{AB}^{\vec{u}} = \tilde{\mathbf{M}}_A^{u_1} \otimes \tilde{\mathbf{M}}_B^{u_2}$. Here, the tilde notation emphasizes that each of the above subsets of POVMs is not normalized, and so, $\tilde{p}(x,y|\vec{u}) = Tr[(\tilde{\mathbf{A}}_x^{u_1} \otimes \tilde{\mathbf{B}}_y^{u_2})\rho_{AB}]$ does not add up to one. Indeed, the sum, $\sum_{X_{u_1}, Y_{u_2}} \tilde{p}(x,y|\vec{u}) = p(\vec{u})$ is the probability of announcing $\vec{u}$.

Taking into account the announcement step, the ccq-density matrix in Equation 5.18 is rewritten as

$$\begin{aligned} \rho_{XYE} &= \sum_{\vec{u}} p(\vec{u}) \quad \left(\sum_{X_{u_1}, Y_{u_2}} p(x,y|\vec{u}) \; |xy\rangle\langle xy|_{AB} \otimes \rho_E^{x,y|\vec{u}} \right) \otimes |\vec{u}\rangle\langle\vec{u}|_C \\ &= \sum_{\vec{u}} p(\vec{u}) \quad \left(\qquad\qquad \rho_{XYE}^{\vec{u}} \qquad\qquad \right) \otimes |\vec{u}\rangle\langle\vec{u}|_C. \end{aligned} \tag{5.29}$$

Here, we replaced $\sum_{X,Y}$ with $\sum_{\vec{u}} \sum_{X_{u_1}, Y_{u_2}}$ and included an extra register C, which stores the classical information that is known to public. In addition, $p(x,y|\vec{u})$ is a normalized conditional joint

statistical distribution and $\rho_E^{x,y|\vec{u}}$ is Eve's conditional quantum state that are given by

$$\begin{aligned} p(x,y|\vec{u}) &= \frac{\tilde{p}(x,y|\vec{u})}{p(\vec{u})}, \\ \rho_E^{x,y|\vec{u}} &= \frac{1}{\tilde{p}(x,y|\vec{u})} Tr_{AB}[(\tilde{\mathbf{A}}_x^{u_1} \otimes \tilde{\mathbf{B}}_y^{u_2} \otimes \mathbb{1})|\Psi\rangle\langle\Psi|_{ABE}]. \end{aligned} \tag{5.30}$$

So far, the announcement is treated as a classical post-processing step, but in the following we show that one can treat this step quantum mechanically by introducing an *announcement map* that is applied *before* the measurements take place. Afterwards, the users perform an *adaptive* measurement for *each* announcement. The reason that these two approaches are theoretically equivalent is that the measurement and the announcement are two independent processes, and therefore, they commute with each other. As long as the statistics $p(x,y|\vec{u})$ are identical in either approach, one can choose one way or another for fitting the announcement step into the security proof formalism.

The author of [93] provides a quantum description of the announcement step by introducing a set of Kraus operators

$$\mathbf{K}_{\vec{u}} := \sqrt{\sum_{X_{u_1}} \mathscr{A}_x} \otimes \sqrt{\sum_{Y_{u_2}} \mathscr{B}_y}. \tag{5.31}$$

which maps the joint quantum state $|\Psi\rangle_{ABE}$ to the announcement subspace by $|\Psi^{\vec{u}}\rangle_{ABE} = \frac{1}{\sqrt{p(\vec{u}}} \mathbf{K}_{\vec{u}} |\Psi\rangle_{ABE}$ where $p(\vec{u}) = Tr[\mathbf{K}_{\vec{u}}|\Psi\rangle\langle\Psi|\mathbf{K}_{\vec{u}}^\dagger]$ is the probability of announcing $\vec{u}$. This is a pure state because we assume Eve has access to the classical information $\vec{u}$ *before* her attack, which is in Eve's favour. Therefore, condition on $\vec{u}$, the announcement followed by Eve's attack transforms the joint quantum state of Alice and Bob to

$$\begin{aligned} \mathscr{E}_{\vec{u}}[|\Phi\rangle\langle\Phi|_{AA'}] &= \frac{1}{p(\vec{u}} Tr_E[\mathbf{K}_{\vec{u}} |\Psi\rangle\langle\Psi|_{ABE} \mathbf{K}_{\vec{u}}^\dagger] \\ &= Tr_E[|\Psi^{\vec{u}}\rangle\langle\Psi^{\vec{u}}|_{ABE}] \\ &= \rho_{AB}^{\vec{u}}. \end{aligned} \tag{5.32}$$

Then, the legitimate users carry out a local measurement *adaptively* with a set of *adaptive* POVMs that are defined in [93],

$$\begin{aligned} \mathbf{M}_A^{u_1} &= \{\mathbf{A}_x^{u_1} := \frac{\mathscr{A}_x}{\sum_{X_{u_1}} \mathscr{A}_x} | x \in X_{u_1}\}, \\ \mathbf{M}_B^{u_2} &= \{\mathbf{B}_y^{u_2} := \frac{\mathscr{B}_y}{\sum_{Y_{u_2}} \mathscr{B}_y} | y \in Y_{u_2}\}. \end{aligned} \tag{5.33}$$

These adaptive measurements result in classical data X_{u_1} and Y_{u_2}. Note that each of the above POVMs satisfies the normalization condition, i.e., $\sum_{X_{u_1}} \mathbf{A}_x^{u_1} = \mathbb{1}$ and $\sum_{Y_{u_2}} \mathbf{B}_y^{u_2} = \mathbb{1}$.

These *adaptive measurements*, denoted by $\mathbf{M}_{AB}^{\vec{u}} = \mathbf{M}_A^{u_1} \otimes \mathbf{M}_B^{u_2}$, yield a conditional ccq-density matrix $\rho_{XYE}^{\vec{u}} \equiv \{|\Psi^{\vec{u}}\rangle_{ABE},\ \mathbf{M}_{AB}^{\vec{u}}\}$, which is equivalent to $\rho_{XYE}^{\vec{u}} \equiv \{|\Psi\rangle_{ABE},\ \tilde{\mathbf{M}}_{AB}^{\vec{u}}\}$ that was obtained from the classical approach. This implies that the quantum description and the classical description of the announcement step yield identical conditional probability distributions, $p(x,y|\vec{u})$, and hence, the two approaches are theoretically equivalent. Therefore, for the rest of this chapter, we conventionally choose the quantum mechanical description of the announcement step, since it is more convenient to use in feature security analysis.

On average, the announcement map and Eve's attack transform the joint quantum states as

$$\begin{aligned} |\Psi\rangle_{ABE} &= \sum_{\vec{u}} \sqrt{p(\vec{u})}\ |\Psi^{\vec{u}}\rangle_{ABE} \otimes |\vec{u}\rangle_C, \\ \bar{\rho}_{AB} &= \sum_{\vec{u}} p(\vec{u})\ \rho_{AB}^{\vec{u}} \otimes |\vec{u}\rangle\langle\vec{u}|_C \end{aligned} \tag{5.34}$$

where the over bar notation reminds the averaging. Accordingly, the average of the mutual information and the Holevo quantity is

$$\begin{aligned} \bar{I}(X:Y) &= \sum_{\vec{u}} p(\vec{u})\ I(X:Y|\vec{u}) + H(p(\vec{u})) \\ \bar{\chi}(\{\rho_{AB},\ \mathbf{M}_{AB}\}) &= \sum_{\vec{u}} p(\vec{u})\ \chi(\{\rho_{AB}^{\vec{u}},\ \mathbf{M}_{AB}^{\vec{u}}\}) + H(p(\vec{u})). \end{aligned} \tag{5.35}$$

Note that the extra term $H(p(\vec{u}))$ appears as a result of the classical information that is broadcast publicly but it will be cancelled out in the key rate. The conditional mutual information is computed by replacing $p(x,y|\vec{u})$ in Equation 5.6. The computation of the conditional Holevo quantity, however, requires more attention, because the quantum state $\rho_{AB}^{\vec{u}}$ that is compatible with the observed data, i.e., $\rho_{XY}^{\vec{u}} \equiv \{\rho_{AB}^{\vec{u}},\ \mathbf{M}_{AB}^{\vec{u}}\}$, is not unique.

Definition 5.4. The subset $\Gamma_{XY}^{\vec{u}} \subset \Gamma_{XY} \subset \Gamma(\mathscr{H}_{AB})$ is a set of all density matrices that are compatible with the conditional statistical information $p(X,Y|\vec{u})$ due to the adaptive measurements $\mathbf{M}_{AB}^{\vec{u}} = \{\mathbf{A}_x^{u_1} \otimes \mathbf{B}_y^{u_2}\}$ such that

$$\Gamma_{XY}^{\vec{u}} = \{\rho_{AB} \in \Gamma(\mathscr{H}_{AB}) \mid p(x,y|\vec{u}) = Tr[(\mathbf{A}_x^{u_1} \otimes \mathbf{B}_y^{u_2})\ \rho_{AB}]\}. \tag{5.36}$$

Therefore, to find the lower bound on the average key rate, the Holevo quantity is maximized

over the subset $\Gamma_{XY}^{\vec{u}}$,

$$\begin{aligned} \bar{R} &\geq \sum_{\vec{u}} p(\vec{u}) \inf_{\rho^{\vec{u}} \in \Gamma_{XY}^{\vec{u}}} R^{\vec{u}} \\ &= \sum_{\vec{u}} p(\vec{u}) \left(I(X:Y|\vec{u}) - \max_{\rho^{\vec{u}} \in \Gamma_{XY}^{\vec{u}}} \chi(\{\rho_{AB}^{\vec{u}}, \mathbf{M}_{AB}^{\vec{u}}\}) \right). \end{aligned} \tag{5.37}$$

In the above description of announcement, we have not considered any *post-selection* step. An example of post-selection is the *sifting* step of the BB84 protocol, where the legitimate users keep only those data that their basis information matches. In that case, it is required to renormalize the density matrices and the probabilities, because part of the data is *filtered*. However, not all announcements involve a post-selection step. One example is the announcement strategy in our proposed STR protocol, which will be explained in detail later.

To clarify each step of a QKD protocol and the notation that was introduced, we elaborate on a well-known example of 6-state protocol in the next section.

5.6 Key Rate of 6-state Protocol

In a 6-state protocol, Alice generates a random number $d_A \in \{0,1\}$ and chooses a basis $u_A \in \{X,Y,Z\}$ with probability $p(u_A)$. She then encodes the classical information $x = (d_A, u_A)$ into a quantum signal $|x\rangle \in \{|0\rangle_{u_A}, |1\rangle_{u_A}\}$ and sends it to Bob. A basis u refers to the eigenstates of the Pauli operator σ_u, with $\alpha \in \{x,y,z\}$, for example, $|0\rangle_X = |+\rangle$. On the other side of the channel, Bob receives a noisy quantum state ρ_B^x and with probability $p(u_B)$ measures his register in basis $u_B \in \{X,Y,Z\}$, resulting in an outcome $d_B \in \{0,1\}$. Assuming that Alice has access to a totally random number generator, we have $p(d_A) = \frac{1}{2}$, and using the source replacement scheme in Equation 5.15, the initial joint quantum state prior to Eve's attack is

$$|\Phi\rangle_{AB} = \sum_{u_A,u_B} \sqrt{p(u_A)\, p(u_B)}\, \frac{(|0\rangle_{u_A}|0\rangle_{u_B} + |1\rangle_{u_A}|1\rangle_{u_B})}{\sqrt{2}} \tag{5.38}$$

In the absence of noise, Alice's and Bob's data are perfectly correlated when their basis matches. Thus, the legitimate users announce their basis information and post select those events that $u_A = u_B = u$. Therefore, $|\Phi\rangle_{AB} = \sum_u \sqrt{p(u)}\, |\Phi^u\rangle_{AB}$ [96], where $|\Phi^{u=Z,X}\rangle = |\phi^+\rangle$, and $|\Phi^{u=Y}\rangle = |\phi^-\rangle$,

where $|\phi^{\pm}\rangle$ is one of the Bell states that are defined in the Z basis as

$$\begin{aligned} |\phi^{+}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\phi^{-}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\psi^{+}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\psi^{-}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{5.39}$$

In the presence of noise, according to the discussion in Section 5.5.3, the announcement followed by Eve's attack maps the initial state to $\mathscr{E}_{\vec{u}}[|\Phi\rangle\langle\Phi|_{AB}] = \rho^{u}_{AB}$. This noisy quantum state results in a basis dependent error rate that is defined by

$$e_u = p(d_A \neq d_B|u) = Tr[(|01\rangle\langle 01|_u + (|10\rangle\langle 10|_u)\ \rho^{u}_{AB}]. \tag{5.40}$$

As discussed before, the quantum state ρ^{u}_{AB} that is compatible with Alice and Bob's observations is not unique. Nevertheless, it is shown in [97, 98] that the optimum attack corresponds to a *Bell diagonal* state which is defined by

$$\begin{aligned} \rho^{u}_{\text{Bell}} &= \delta_1\ |\phi^{+}\rangle\langle\phi^{+}|_u + \delta_2\ |\phi^{-}\rangle\langle\phi^{-}|_u + \delta_3\ |\psi^{+}\rangle\langle\psi^{+}|_u + \delta_4\ |\psi^{-}\rangle\langle\psi^{-}|_u \\ &= \sum_i \delta_i\ |\phi^{i}\rangle\langle\phi^{i}|_u \end{aligned} \tag{5.41}$$

Hence, to lower bound the key rate, we need to optimize with respect to a smaller subset $\Gamma^{u}_{\text{Bell}} = \{\rho^{u}_{\text{Bell}}\}$ rather than Γ^{u}_{XY}. Thus, the Holevo quantity in Equation 5.24 becomes

$$\begin{aligned} \bar{\chi}(X:E) &\leq \sum_u p(u)\ \max_{\Gamma^{u}_{\text{Bell}}}\ \{\ S(\rho^{u}_{AB}) - \sum_{d_A} p(d_A|u)\ S(\rho_B^{d_A|u})\} \\ &= -\sum_u p(u)\ \max_{\Gamma^{u}_{\text{Bell}}}\{Tr[\rho^{u}_{\text{Bell}}\ \log\rho^{u}_{\text{Bell}}] - \frac{1}{2}\sum_{d_A} Tr[\rho_B^{d_A|u}\ \log\rho_B^{d_A|u}\} \end{aligned} \tag{5.42}$$

in which $p(d_A|u) = \frac{1}{2}$ and the conditional reduced density matrix is $\rho_B^{d_A|u} = \frac{1}{p(d_A|u)} Tr_A[(|d_A\rangle\langle d_A| \otimes \mathbb{1})\ \rho^{u}_{\text{Bell}}]$. For example, for $u = Z$ basis, that reduced state is

$$\begin{aligned} \rho_B^{d_A=0|u=Z} &= (\delta_1+\delta_2)|0\rangle\langle 0| + (\delta_3+\delta_4)|1\rangle\langle 1|, \\ \rho_B^{d_A=1|u=Z} &= (\delta_1+\delta_2)|1\rangle\langle 1| + (\delta_3+\delta_4)|0\rangle\langle 0|. \end{aligned} \tag{5.43}$$

To upper bound Eve's knowledge, Alice and Bob require to use their statistical information, $p(d_A, d_B|u)$, and characterize ρ^u_{Bell}, or equivalently compute the δ_i parameters. They may need to optimize the key rate with respect to the free (unknown) parameters, but in particular case of 6-state protocol, no further optimization is required. Because, the measurement bases are topographically complete, and hence, the basis dependent error rates

$$\begin{aligned} e_x &= (\delta_2 + \delta_4) \\ e_y &= (\delta_2 + \delta_3) \\ e_z &= (\delta_3 + \delta_4) \end{aligned} \tag{5.44}$$

along with the normalization condition, $\sum_i \delta_i = 1$, are enough to fully characterize the Bell diagonal state or to compute all δ_i. Explicitly,

$$\begin{aligned} \delta_1 &= 1 - \frac{1}{2}(e_x + e_y + e_z), \\ \delta_2 &= \frac{1}{2}(e_x + e_y - e_z), \\ \delta_3 &= \frac{1}{2}(e_y + e_z - e_x), \\ \delta_4 &= \frac{1}{2}(e_z + e_x - e_y). \end{aligned} \tag{5.45}$$

Therefore, once the error rates are estimated in the PE step, Alice and Bob are able to compute the upper bound on the Holevo quantity via Equation 5.42 and obtain

$$\bar{\chi}(X:E) = (-\sum_i \delta_i \log \delta_i) + \sum_u p(u)\, h(e_u). \tag{5.46}$$

Here, $h(x) = -x\log(x) - (1-x)\log(1-x)$ is the binary entropy.

To computation the mutual information, we substitute $p(d_A, d_B|u)$ into the definition in Equation 5.6, and replace $p(d_A|u) = p(d_B|u) = \frac{1}{2}$ and $p(d_A = d_B|u) = \frac{1}{2}(1-e_u)$ to obtain

$$\begin{aligned} I(X:Y) &= H(X) - H(X|Y) \\ &= -\sum_u \sum_{d_A, d_B} p(u)\, (2\, p(d_A|u)\, \log p(d_A|u) - \, p(d_A, d_B|u)\, \log p(d_A, d_B|u) \\ &= \sum_u p(u)(1 - h(e_u)) \end{aligned} \tag{5.47}$$

Finally, the lower bound on the average key rate of 6-state protocol is

$$\overline{R}_{\text{6-state}} \geq \sum_u p(u)\, (1 - 2\, h(e_u)) + (\sum_i \delta_i \log \delta_i), \tag{5.48}$$

where the δ_i are substitute from Equation 5.45.

In case of BB84 protocol, the calculation is more complicated. The reason is that in BB84, the measurement bases, $\{X,Z\}$, are not topographically complete, and hence, there is a degree of freedom in e_y. Therefore, the density matrix ρ^u_{Bell} is not uniquely determined from the observations and one needs to use this degree of freedom in such a way to maximize Eve's information. The authors of [99, 100] have done the optimization for the case of direct link QKD and obtained

$$\overline{R}_{BB84} \geq \sum_u p(u)\ (1-2\,h(e_u)). \tag{5.49}$$

Comparing the two key rates, we conclude that the 6-state protocol has a larger key than the BB84 protocol.

5.7 Security Proof of Simplified Trusted Relay Protocol

In previous sections, we provided the standard formalism for the security proof of QKD protocols. In this section, we adopt this formalism and apply it to our proposed QKD protocol and prove its security.

A simplified trusted relay (STR) consists of at least 3 users in a quantum network: Alice and Bob are the legitimate users, and an intermediate trusted node, named T-node. Alice and Bob communicate with the T-node independently, through links a and b, and there is no direct quantum communication between them. In the source replacement scheme or in Entanglement Based (EB) QKD, each one of Alice and Bob prepares an entangled state, keeps the first qubit, A or B, for themselves, and sends the other qubit, A' or B', to the T-node via a noisy quantum channel monitored by Eve. In Eve's attack, she attaches an ancillary register E' to the flying qubits, A' and B', and operates a unitary transformation on the composite system, $U_{A'B'E'\to T_aT_bE}$. The transformed noisy qubits, T_a and T_b, arrive at the T-node's laboratory and are measured afterwards. Once the states are distributed, Alice and Bob carry out their local measurements on their qubits, resulting in classical data $x=(d_A,u_A)$ and $y=(d_B,u_B)$, which are uncorrelated at this stage. The first bit of data contains the raw key information and the second bit contains the basis information. Similarly, the T-node carries out two local measurements on the two noisy signals, resulting in two pairs of classical data, $\vec{s}=(s_a,s_b)$, with $s_a=(d_a,u_a)$ and $s_b=(d_b,u_b)$. The quantum phase of a STR protocol is no different from a conventional trusted relay, where the quantum signals are distributed and measured, and Eve's attack occurs. Figure 5.1 pictorially demonstrates this phase.

In the classical phase of a STR protocol, two types of announcements take place that eventually result in a direct classical correlation between Alice's data and Bob's data. The first type

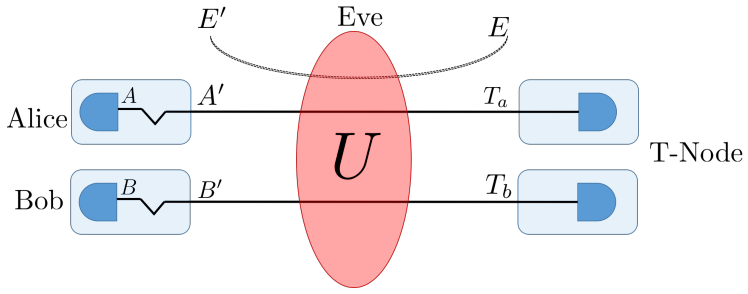

Figure 5.1: Distribution and Measurement Steps of a Simplified Trusted Relay Protocol: Alice (Bob) keeps the first qubit of the quantum state $|\Phi\rangle$ (represented by solid lines) and sends the second qubit A' (B') to the T-node. Eve interacts with the flying qubits by a unitary transformation U and sends the transformed qubits, T_a and T_b, to the T-node where they are measured. Each measurement is denoted by a solid semicircle.

is the *basis* announcement made by all users in the network which leads to filtering part of the data. The second type is the *parity* announcement made by the T-node which results in a direct correlation between the legitimate users' data and is the novelty of the present work.

In the following, we provide a mathematical description for each step of the above scenario and analytically compute the lower bound on the key rate of a STR protocol. We treat the announcement steps as quantum mechanical maps, based on the argument in Section 5.5.3, and show that the parity announcement creates enough correlation between Alice's and Bob's data to proceed with error correction and privacy amplification step by themselves and no further action from the T-node is required.

5.7.1 Quantum State Distribution

In the source replacement scheme, the legitimate users prepare $|\varphi_x\rangle$ and $|\varphi_y\rangle$ with probabilities $p(x)$ and $p(y)$ respectively. In the absence of Eve's attack, the initial state is

$$|\Phi\rangle_0 := |\Phi\rangle_{ABA'B'} = \sum_{X,Y} \sqrt{p(x)}\,\sqrt{p(y)}\,|xy\rangle_{AB} \otimes |\varphi_x\rangle_{A'} \otimes |\varphi_y\rangle_{B'}. \tag{5.50}$$

Due to the presence of an eavesdropper on the channel, the flying qubits A' and B' will not arrive at the destination safely. Eve's attack is described by a unitary transformation $U_{A'B'E'\to T_aT_bE}$, applied on the composite system of the flying qubits, A' and B', and Eve's ancillary register, E'. Note that $\dim(\mathscr{H}_{E'}) = \dim(\mathscr{H}_{A'B'})$. After the attack, Eve resends the transformed qubits,

$T = T_a T_b$, to the T-node. Therefore, the outcome of the noisy quantum channel is

$$\begin{aligned} |\Psi\rangle_{ABTE} &= (\mathbb{1}_{AB} \otimes U_{A'B'E' \to T_a T_b E})(|\Phi\rangle_0 \otimes |E'\rangle), \\ &= \sum_{X,Y} \sqrt{p(x)}\ \sqrt{p(y)}\ |x\,y\rangle_{AB} \otimes |\psi^{x,y}\rangle_{TE} \end{aligned} \tag{5.51}$$

According to the system-environment representation, the reduced system transforms by a CPTP map given by

$$\begin{aligned} \rho_{ABT} &= Tr_E[|\Psi\rangle\langle\Psi|_{ABTE}] = (\mathbb{1}_{AB} \otimes \mathscr{E})[|\Phi\rangle\langle\Phi|_0], \\ &= \sum_{X,Y} p(x)\ p(y)\ |x\,y\rangle\langle x\,y|_{AB}\ \otimes\ \rho_T^{x,y}, \end{aligned} \tag{5.52}$$

where

$$\begin{aligned} \rho_T^{x,y} &= Tr_E\left[|\psi^{x,y}\rangle\langle\psi^{x,y}|_{TE}\right], \\ &= \mathscr{E}\left[|\varphi_x\rangle\langle\varphi_x|_{A'} \otimes |\varphi_y\rangle\langle\varphi_y|_{B'}\right]. \end{aligned} \tag{5.53}$$

Eve's attack is thus characterized either by a unitary, U, in a larger Hilbert space or by a quantum CPTP map $\mathscr{E}_{A'B' \longmapsto T_a T_b}$ on the reduced system. Furthermore, according to the Choi-Jamiolkowski isomorphism, the characterization of the noisy quantum channel, $\mathscr{E}$, is equivalent to the characterization of the noisy quantum state, ρ_{ABT}.

Note that Alice and Bob's reduced density matrix is a product state, $\rho_A \otimes \rho_B = Tr_T[\rho_{ABT}]$, which confirms that their data are uncorrelated.

5.7.2 Measurements

Each user in the network measures its qubits and obtains classical data: Alice and Bob measurements are described by POVMs, $\mathbf{M}_{AB} = \{\mathscr{A}_x \otimes \mathscr{B}_y\}$, resulting in classical data $X = \{x\}$ and $Y = \{y\}$ and the T-node's measurements are described by POVMs, $\mathbf{M}_T = \{\mathtt{T}_{s_a}^{(a)} \otimes \mathtt{T}_{s_b}^{(b)}\}$, resulting in classical data $S = \{(s_a, s_b)\}$. The upper index of the T-node's measurement operators refers to the link index, a or b. The joint classical information is described by

$$\rho_{XYS} = \sum_{X,Y,S} p(x,y,\vec{s})\ |x\,y\rangle\langle x\,y|\ \otimes\ |\vec{s}\rangle\langle\vec{s}|, \tag{5.54}$$

in which $p(x,y,\vec{s})$ is the statistical information and is given by

$$p(x,y,\vec{s}) = Tr[(\mathscr{A}_x \otimes \mathscr{B}_y \otimes \mathtt{T}_{s_a}^{(a)} \otimes \mathtt{T}_{s_b}^{(b)})\ \rho_{ABT}]. \tag{5.55}$$

Since Alice's and Bob's data are uncorrelated according to Equation 5.52, their joint statistical information has a product form, $p(x,y,\vec{s}) = p(x,\vec{s})\ p(y,\vec{s})$

Like before, we denote the subset $\Gamma_0 \subset \Gamma(\mathscr{H}_{ABT})$ as a set of all four-party density matrices, ρ_{ABT}, that are compatible with Alice, Bob and the T-node's statistical information, $p(X,Y,S) \equiv \rho_{XYS} \equiv \{\rho_{ABT}\ ,\ \mathbf{M}_{AB} \otimes \mathbf{M}_T\}$.

5.7.3 Basis Announcement

Like most conventional QKD protocols, in a STR network, Alice, Bob and the T-node announce the basis information, $(u_A,\ u_B,\ (u_a,\ u_b))$, publicly and post-select those events that their basis information matches and ignore the rest. Explicitly, the two pairs of raw key data, (d_A,d_a), from link a, and (d_B,d_b), from link b, are stored only if $(u_A = u_a := u_1)$ and $(u_B = u_b := u_2)$. According to Section 5.5.3, this public announcement repartitions the observed data as

$$\begin{aligned} X_{u_1} &= \{\, x \in X \,|x = (d_A,u_1)\,\}, \\ Y_{u_2} &= \{\, y \in Y \,|y = (d_B,u_2)\,\}, \\ S_{\vec{u}} &= \{\, (s_a,s_b) \in S \,|s_a = (d_a,u_1)\ \&\ s_b = (d_b,u_2)\,\}, \end{aligned} \tag{5.56}$$

where $\vec{u} = (u_1,u_2)$. In the quantum mechanical approach, the basis announcement is described by a quantum map with Kraus operators

$$\mathbf{K}_{\vec{u}} := \sqrt{\sum_{X_{u_1}} \mathscr{A}_x} \otimes \sqrt{\sum_{Y_{u_2}} \mathscr{B}_y} \otimes \sqrt{\sum_{S_{\vec{u}}} \mathtt{T}_{s_a}^{(a)} \otimes \mathtt{T}_{s_b}^{(b)}}. \tag{5.57}$$

Correspondingly, the noisy joint quantum states in Equation 5.51 and Equation 5.52 are rewritten as

$$\begin{aligned} |\Psi\rangle_{ABTE} &= \sum_{\vec{u}} \sqrt{p(\vec{u})}\ |\Psi^{\vec{u}}\rangle_{ABTE} \otimes |\vec{u}\rangle_C, \\ \rho_{ABT} &= \sum_{\vec{u}} p(\vec{u})\ \rho_{ABT}^{\vec{u}} \otimes |\vec{u}\rangle\langle\vec{u}|_C, \end{aligned} \tag{5.58}$$

where for a given $\vec{u}$, the conditional reduced density matrix of all users in the network is $\rho_{ABT}^{\vec{u}} = \frac{1}{\tilde{p}(\vec{u})}(\mathbf{K}_{\vec{u}}\ \rho_{ABT}\ \mathbf{K}_{\vec{u}}^{\dagger})$ with the normalization factor $\tilde{p}(\vec{u}) = Tr[\mathbf{K}_{\vec{u}}\ \rho_{ABT}\ \mathbf{K}_{\vec{u}}^{\dagger}]$. Here, the information stored in the classical register C, is accessible to everyone, including Eve. It is important to note that since the data are post-selected, the probabilities must be renormalized. Indeed, the probability of keeping the data is $p_{\text{keep}} = \sum_{\vec{u}} \tilde{p}(\vec{u})$, and thus, $p(\vec{u}) = \frac{\tilde{p}(\vec{u})}{p_{\text{keep}}}$. Additionally, because

the basis announcements in links a and b are based on local randomness, it is expected that $p(\vec{u}) = p(u_1)\ p(u_2)$. The final remark here is that the joint state $|\Psi^{\vec{u}}\rangle_{ABTE}$ is a pure state, because we assume Eve's attack takes place *after* the basis announcement, which is an assumption in Eve's favour.

For a given $\vec{u}$, the corresponding adaptive measurement operators are $\mathbf{M}_{AB}^{\vec{u}} = \mathbf{M}_A^{u_1} \otimes \mathbf{M}_B^{u_2}$ for the legitimate users, and $\mathbf{M}_T^{\vec{u}}$ for the T-node. The definition of $\mathbf{M}_{AB}^{\vec{u}}$ is given in Equation 5.33 and

$$\mathbf{M}_T^{\vec{u}} \quad = \quad \{\mathbf{T}_{\vec{s}}^{\vec{u}} := \frac{\mathrm{T}_{s_a}^{(a|u_1)} \otimes \mathrm{T}_{s_b}^{(b|u_2)}}{\sum\limits_{S_{\vec{u}}} \mathrm{T}_{s_a}^{(a|u_1)} \otimes \mathrm{T}_{s_b}^{(b|u_2)}} | (s_a, s_b) \in S_{\vec{u}} \ \& \ \mathrm{T}_{s_a}^{(a)} \otimes \mathrm{T}_{s_b}^{(b)} \in \mathbf{M}_T \}. \tag{5.59}$$

Correspondingly, these measurements result in the conditional statistical information $p(x,y,\vec{s}|\vec{u})$. The subset $\Gamma^{\vec{u}} \subset \Gamma_0$ contains all four-party density matrices that are compatible with Alice, Bob and the T-node's statistical informations, $\rho_{XYS}^{\vec{u}} \equiv \{\rho_{ABT}^{\vec{u}}\ ,\ \mathbf{M}_{AB}^{\vec{u}} \otimes \mathbf{M}_T^{\vec{u}}\}$.

It is very important to note that the basis announcement correlates the data of each legitimate user with the T-node's data respectively, but no correlation with themselves, meaning that the reduced density matrix of Alice and Bob is still a product state, i.e., $\rho_A^{u_1} \otimes \rho_B^{u_2} = Tr_T[\rho_{ABT}^{\vec{u}}]$ or equivalently, $p(x,y,\vec{s}|\vec{u}) = p(x,\vec{s}|\vec{u})\ p(y,\vec{s}|\vec{u})$. Here is when the novelty of our announcement strategy comes in to create correlation between Alice's and Bob's data.

5.7.4 Parity Announcement

In the *parity* announcement, which differentiates a STR network from a traditional trusted relay networks, the T-node announces the bitwise parity of each instances of its raw key data denoted by $\lambda = (d_a \oplus d_b)$. Within the subspace of matched bases, $\vec{u}$, the *parity* announcement is described by a quantum map with Kraus operators

$$\mathbf{K}_{\vec{u}}^{\lambda} = \mathbb{1}_{AB} \otimes \sqrt{\sum_{s_a=(d_a,u_1)} \sum_{s_b=(d_a\oplus\lambda,u_2)} \mathrm{T}_{s_a}^{(a)} \otimes \mathrm{T}_{s_b}^{(b)}}. \tag{5.60}$$

Correspondingly, the noisy joint quantum states in Equation 5.58 are rewritten as

$$\begin{aligned} |\Psi\rangle_{ABTE} \quad &= \quad \sum_{\vec{u},\lambda} \sqrt{p(\vec{u})} \sqrt{p(\lambda|\vec{u})}\ |\Psi^{\lambda|\vec{u}}\rangle_{ABTE} \otimes |\vec{u}\lambda\rangle_C, \\ \rho_{ABT} \quad &= \quad \sum_{\vec{u},\lambda} p(\vec{u})\ p(\lambda|\vec{u})\ \rho_{ABT}^{\lambda|\vec{u}} \otimes |\vec{u}\lambda\rangle\langle\vec{u}\lambda|_C, \end{aligned} \tag{5.61}$$

where $\rho_{ABT}^{\lambda|\vec{u}} = (\mathbf{K}_{\vec{u}}^{\lambda}\ \rho_{ABT}^{\vec{u}}\ \mathbf{K}_{\vec{u}}^{\lambda\dagger})/p(\lambda|\vec{u})$ is the noisy quantum state of all users conditioned on the basis and parity announcements and $p(\lambda|\vec{u}) = Tr[\mathbf{K}_{\vec{u}}^{\lambda}\ \rho_{ABT}\ \mathbf{K}_{\vec{u}}^{\lambda\dagger}]$ is the probability of parity announcement within the basis selected subspace.

We highlight on two crucial points here:

1. Once the bitwise parity information is announced by the T-node, the conditional reduced density matrix of Alice and Bob, $\rho_{AB}^{\lambda|\vec{u}} = Tr_T[\rho_{ABT}^{\lambda|\vec{u}}]$, is no longer in a product form meaning that the legitimate users' data is correlated. Consequently, Alice and Bob can proceed with the other classical data processing steps by themselves and no further contribution from the intermediate node is required. The T-node still needs to cooperates with the legitimate users in the PE step in order to characterize $\rho_{ABT}^{\lambda|\vec{u}}$.

2. In contrast to the conventional QKD schemes, in a STR protocol, the reduced density matrix of Alice, Bob and Eve is not a pure state,

$$\rho_{ABE}^{\lambda|\vec{u}} \quad = \quad Tr_T[\ |\Psi^{\lambda|\vec{u}}\rangle\langle\Psi^{\lambda|\vec{u}}|_{ABTE}]. \tag{5.62}$$

   This implies that there is some quantum information that are *hidden* to Eve. In other words, because Eve does not have access to the T-node's laboratory, the quantum registers T_a and T_b are inaccessible to her. Consequently, even though the bitwise parity λ and the basis information $\vec{u}$ is known publicly, the individual data, s_a and s_b, are unknown to Eve. Non-purity of $\rho_{ABE}^{\lambda|\vec{u}}$ also implies that T-node needs to collaborate with Alice and Bob in the PE step because the the T-node has some information that no one else has, but, no further collaboration is required in the EC and the PA steps.

For given $\vec{u}$ and λ, the corresponding adaptive measurements are $\mathbf{M}_{AB}^{\vec{u}} \otimes \mathbf{M}_{T}^{\lambda|\vec{u}}$, leading to a classical density matrix,

$$\begin{aligned} \rho_{XYS}^{\lambda|\vec{u}} \quad &\equiv \quad \{\rho_{ABT}^{\lambda|\vec{u}}\ ,\ \mathbf{M}_{AB}^{\vec{u}} \otimes \mathbf{M}_{T}^{\lambda|\vec{u}}\}, \\ \mathbf{M}_{T}^{\lambda|\vec{u}} \quad &:= \quad \{\mathbf{T}_{\vec{s}}^{\vec{u}} \in \mathbf{M}_{T}^{\vec{u}}|\ s_a \oplus s_b = \lambda\}. \end{aligned} \tag{5.63}$$

The above adaptive measurements result in the conditional joint statistical distribution $p(x,y,\vec{s}|\vec{u},\lambda)$ which admits correlation between Alice's and Bob's data.

5.7.5 Summary and the Key Rate

In the above sections, we broke a STR protocol to three stages: The first stage involves only the Eve's attack; The second stage involves the basis announcement followed by Eve's attack;

And, the last stage involves the basis and parity announcement followed by Eve's attack. For each stage, we provided a description of the corresponding quantum maps and the noisy joint quantum states as well as the joint statistical information that is obtained once the adaptive measurements take place. This is summarized as

$$
\begin{aligned}
|\Phi\rangle_0 \otimes |E'\rangle \quad &\xrightarrow{\text{Eve's attack}} \quad |\Psi\rangle_{ABTE} \xrightarrow{\mathbf{M}_{AB} \otimes \mathbf{M}_T} p(x,\vec{s})p(y,\vec{s}), \\
|\Psi\rangle_{ABTE} \quad &\xrightarrow{+\text{Basis annc.}} \quad \sum_{\vec{u}} \sqrt{p(\vec{u})}\, |\Psi^{\vec{u}}\rangle_{ABTE} \otimes |\vec{u}\rangle_C \xrightarrow{\mathbf{M}^{\vec{u}}_{AB} \otimes \mathbf{M}^{\vec{u}}_T} p(x,\vec{s}|\vec{u})p(y,\vec{s}|\vec{u}), \\
|\Psi^{\vec{u}}\rangle_{ABTE} \quad &\xrightarrow{+\text{Parity annc.}} \quad \sum_{\lambda} \sqrt{p(\lambda|\vec{u})}\, |\Psi^{\lambda|\vec{u}}\rangle_{ABTE} \otimes |\vec{u}\lambda\rangle_C \xrightarrow{\mathbf{M}^{\vec{u}}_{AB} \otimes \mathbf{M}^{\lambda|\vec{u}}_T} p(x,y,\vec{s}|\vec{u},\lambda).
\end{aligned}
\tag{5.64}
$$

At the end of a STR protocol, an identical and secure key is shared between Alice and Bob at an average rate

$$
\begin{aligned}
\bar{R} &\geq \bar{I}(X:Y) - \max_{\Gamma_0} \bar{\chi}(\rho_{XE}), \\
&\geq \sum_{\vec{u}} p(\vec{u}) \{ \qquad\qquad R_{\vec{u}} \qquad\qquad \}, \\
&= \sum_{\vec{u}} p(\vec{u}) \{ I(X:Y|\vec{u}) - \max_{\Gamma^{\vec{u}}} \chi(\rho^{\vec{u}}_{XE}) \}, \\
&\geq \sum_{\vec{u}} p(\vec{u}) \sum_{\lambda} p(\lambda|\vec{u}) \{ I(X:Y|\lambda,\vec{u}) - \max_{\Gamma^{\lambda|\vec{u}}} \chi(\rho^{\lambda|\vec{u}}_{XE}) \},
\end{aligned}
\tag{5.65}
$$

in which $\Gamma^{\lambda|\vec{u}} \subseteq \Gamma^{\vec{u}} \subseteq \Gamma_0$ defines the set of all density matrices $\rho^{\lambda|\vec{u}}_{ABT}$ that are compatible with the observed data conditioned on the public announcements λ and $\vec{u}$. To obtain the lower bound, we used the convexity property of the mutual information as well as the concavity property of the Holevo quantity [93]. Moreover, in the second line, we introduced $R_{\vec{u}}$ as the key rate in the subspace of the announced $\vec{u}$. Once more, we emphasize that the choice of basis is determined by local randomness, and so, $p(\vec{u}) = p(u_1)p(u_2)$, and the basis announcement does not correlate link a with link b. But, λ is determined by bitwise parity of the outcomes of two measurements, and so, $p(\lambda|\vec{u})$ does not have a product form.

5.8 6-state and BB84 protocols

In previous sections, we demonstrated a formalism for the security of a simplified trusted relay QKD protocol (STR-QKD). In this section we apply this formalism to two well-known examples,

6-state and BB84 protocols, [4] and [101], and derive a numerical lower bound on the secure key rate. In both of these protocols, we consider the ideal case where the legitimate users produce and distribute an unlimited number of single-qubit signals. What follows is valid for both 6-state and BB84 protocols, unless otherwise stated.

According to canonical-source replacement scheme, the initial state prior to Eve's attack is

$$|\Phi\rangle_{AA'BB'} = |\phi^+\rangle_{AA'} \otimes |\phi^+\rangle_{BB'} \tag{5.66}$$

As a starting point and for simplicity in calculation, we assume Eve attacks each link, a and b, independently, meaning that

$$U = U_{AA'E'_a \to AT_aE_a} \otimes U_{BB'E'_b \to BT_bE_b}. \tag{5.67}$$

This assumption sounds very strong and considers a very particular type of attacks. Nevertheless, it will be discussed that the above attack can be used as a building block for deriving the key rate of a more general type of attacks by using the inherent symmetry in 6-state and BB84 protocols.

The two independent collective attacks on links a and b leads to

$$\begin{aligned} |\Phi\rangle_{AA'BB'} &\xrightarrow{U} \rho_{AT_a} \otimes \rho_{BT_b} \\ &= \sum_i \delta_i \, |\phi^i\rangle\langle\phi^i|_{AT_a} \otimes \sum_j \eta_j \, |\phi^j\rangle\langle\phi^j|_{BT_b}, \end{aligned} \tag{5.68}$$

in which $|\phi^i\rangle \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. As discussed before, among all possible quantum states that are compatible with user's observations, the Bell diagonal states corresponds to the optimum attack, [97] and [98], and therefore, in the last line, we replaced the noisy quantum state in each link with the Bell diagonal state.

After the state distribution and Eve's attack, each one of the users in the network measure its qubit(s) with POVMs, $\mathbf{M}_A = \{p(u_A)\ \mathbf{A}_x^{u_A}\}, \mathbf{M}_B = \{p(u_B)\ \mathbf{B}_y^{u_B}\}$ and $\mathbf{M}_T = \{p(u_a)\ p(u_b)\ \mathbf{T}_{s_a}^{u_a} \otimes \mathbf{T}_{s_b}^{u_b}\}$, where

$$\begin{aligned} \mathbf{A}_x^{u_A} &\in \{\ |0\rangle\langle 0|_{u_A},\ |1\rangle\langle 1|_{u_A}\}, \\ \mathbf{B}_y^{u_B} &\in \{\ |0\rangle\langle 0|_{u_B},\ |1\rangle\langle 1|_{u_B}\}, \\ \mathbf{T}_{s_a}^{u_a} \otimes \mathbf{T}_{s_b}^{u_b} &\in \{\ |00\rangle\langle 00|_{u_au_b}, |11\rangle\langle 11|_{u_au_b},\ |01\rangle\langle 01|_{u_au_b},\ |10\rangle\langle 10|_{u_au_b}\}. \end{aligned} \tag{5.69}$$

For clarifications, $|0\rangle_Z = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|0\rangle_X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $|0\rangle_Y = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$ and so forth. Once the basis announcement takes place and the data are post-selected, the adaptive measurements result

in the basis dependent error rates that are given by

$$\begin{aligned} e^a_{u_1} &:= p(d_A \neq d_a,\, u_A = u_a = u_1) = \sum_{x \neq s_a} Tr[(\mathbf{A}^{u_1}_x \otimes \mathbf{T}^{u_1}_{s_a})\, \rho_{AT_a}] \\ e^b_{u_2} &:= p(d_B \neq d_b,\, u_B = u_b = u_2) = \sum_{y \neq s_b} Tr[(\mathbf{B}^{u_2}_y \otimes \mathbf{T}^{u_2}_{s_b})\, \rho_{BT_b}] \end{aligned} \tag{5.70}$$

In the next step, the T-node announces the bitwise parity of each instances of data, where in case of single-qubit signals, the parity bit is either *even* ($\lambda = d_a \oplus d_b = 0$) or *odd* ($\lambda = d_a \oplus d_b = 1$). Therefore, in the subspace of the announced basis, $\vec{u} = (u_1, u_2)$, the Kraus operators associated with the parity announcement map are

$$\begin{aligned} \mathbf{K}^{\text{even}}_{\vec{u}} &= \mathbb{1}_{AB} \otimes (\, |00\rangle\langle 00|_{u_1u_2} + \, |11\rangle\langle 11|_{u_1u_2})^{1/2}, \\ \mathbf{K}^{\text{odd}}_{\vec{u}} &= \mathbb{1}_{AB} \otimes (\, |01\rangle\langle 01|_{u_1u_2}, \, |10\rangle\langle 10|_{u_1u_2})^{1/2}. \end{aligned} \tag{5.71}$$

Consequently, the reduced density matrix of the legitimate users in the network, conditioned on the parity information λ and the basis information $\vec{u}$ is

$$\rho^{\lambda|\vec{u}}_{AB} = Tr_T[\rho^{\lambda|\vec{u}}_{ABT}], \tag{5.72}$$

where

$$\rho^{\lambda|\vec{u}}_{ABT} = \frac{1}{p(\lambda|\vec{u})}(\mathbf{K}^{\lambda}_{\vec{u}}\; SWAP_{T_a \leftrightarrow B}[\, \rho_{AT_a} \otimes \rho_{BT_b}]\; \mathbf{K}^{\lambda\dagger}_{\vec{u}}). \tag{5.73}$$

Here, the $SWAP[.]$ operator ensures that the Hilbert paces are in the right order and has no effect to the security proof. We consider $p(\text{even}|\vec{u}) = p(\text{odd}|\vec{u}) = \frac{1}{2}$ and compute the reduced density matrix of Alice and Bob for $\lambda = \text{even}$, as an example, and obtain

$$\rho^{\text{even}|\vec{u}}_{AB} = \frac{1}{2}[(1-\tilde{e}_{\vec{u}})(|00\rangle\langle 00| + |11\rangle\langle 11|)_{u_1u_2} + \tilde{e}_{\vec{u}}(|01\rangle\langle 01| + |10\rangle\langle 10|)_{u_1u_2}], \tag{5.74}$$

where $\tilde{e}_{\vec{u}} = e^{(a)}_{u_1}(1-e^{(b)}_{u_2}) + e^{(b)}_{u_2}(1-e^{(a)}_{u_1})$ is the *effective* error rate that is a function of errors in each link. In the parameter estimation step, Alice, Bob and the T-node communicate over an authenticated classical channel in order to estimate the basis dependent error rates in each link, $e^{(a)}_{u_1}$ and $e^{(b)}_{u_2}$, by which the reduced density matrix of Alice and Bob in Equation 5.72 is characterized. Given $\rho^{\lambda|\vec{u}}_{AB}$ and the corresponding statistical information $p(x,y|\lambda,\vec{u})$, the average mutual information between Alice and Bob is

$$\begin{aligned} \bar{I}(X:Y) &= \sum_{\vec{u}} p(\vec{u}) \sum_{\lambda \in \{\text{even, odd}\}} p(\lambda|\vec{u}) \left(2 + \sum_{x,y} p(x,y|\lambda,\vec{u})\, \log p(x,y|\lambda,\vec{u})\right) \\ &= \sum_{u_1,u_2 \in \{X,Y,Z\}} p(\vec{u})\, (1 - h(\tilde{e}_{\vec{u}})) \end{aligned} \tag{5.75}$$

The above expression is valid for both 6-state and BB84 protocols. But for computing the Holevo quantity we need to differentiate the two protocols.

5.8.1 Holevo Quantity of the 6-state STR protocol

In order to calculate the Holevo quantity numerically, we consider an asymmetry version of the 6-state protocol, where the most frequent basis, Z, is used for the key generation and the other bases, X and Y are used for the parameter estimation so that $p(u=Z) \gg p(u=X,Y)$. Thus, for simplicity in the notation, we drop the upper index $\vec{u}=(Z,Z)$. We use the definition in Equation 5.24 and replace the density matrices from Equation 5.74 to obtain

$$\begin{aligned}
\bar{\chi}^{\text{6-state}}(X:E) &\leq \sum_{\lambda} p(\lambda)\, \bar{\chi}^{\text{6-state}}(\{\rho^{\lambda}_{ABT}, \mathbf{M}_{AB}\otimes\mathbf{M}^{\lambda}_{T}\}) \\
&= \sum_{\lambda} p(\lambda) \left(S(\rho^{\lambda}_{ABT}) - \sum_{x} p(x|\lambda)\, S(\rho_B^{x|\lambda}) \right) \\
&= -\sum_{ij} \delta_i\, \eta_j\, \log(\delta_i\, \eta_j) - h(e_{\vec{u}}) \\
&= q_z + (1-q_z)\, h\left(\frac{1-(2q_x+q_z)/2}{1-q_z}\right) \\
&:= I_E\,(q_x, q_z)
\end{aligned} \tag{5.76}$$

in which $q_x := e_z^a(1-e_x^b) + e_z^b(1-e_x^a)$ and $q_z := e_z^a + e_z^b - e_z^b e_z^a$ are replaced. Because measurements are topographically complete in case of 6-state protocol, one can fully characterize ρ_{ABT} from the error parameters e_u in each link and no optimization is required.

Eventually, the difference between the mutual information and the Holevo quantity gives the key rate. For a numerical evaluation, we consider $Q = e_x^{a/b} = e_y^{a/b} = e_z^{a/b}$ and obtain

$$\begin{aligned}
\bar{R}_{\infty}^{\text{6-state}} &\geq \bar{I}(X:Y) - \bar{\chi}^{\text{6-state}}(\rho_{XE}) \\
&= 1 - h\,(2Q(1-Q)) - I_E\,(2Q(1-Q), Q(2-Q))
\end{aligned}$$

The key rate of the 6-state STR protocol is plotted in Figure 5.2 as a function of single-link error rate, Q, and is compared with the key rate of the direct link 6-state protocol. The result shows that the simplified trusted relay network, in principle, extends the range of QKD protocols in the expense of reducing the maximum tolerable single link error rate from 12% to 6.5%.

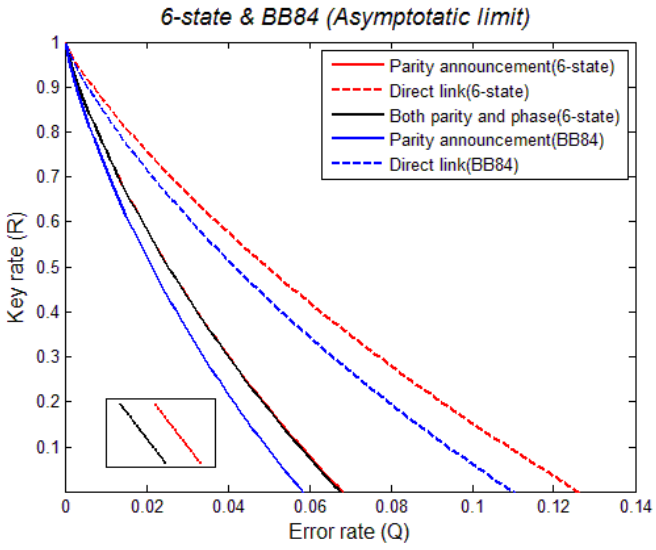

Figure 5.2: Key Rate as a Function of Single-Link Error Rate, Q: Blue lines refer to the BB84 protocol and the red lines correspond to 6-state protocol. The solid lines are plotted in contrast to the dashed lines to show the comparison of this parity announcement strategy in a double-link communication with the key rate of a direct single-link communication.

5.8.2 Holevo Quantity of the BB84 STR protocol

As mentioned in Section 5.6, in case of BB84 protocol, the POVM elements are not topographically complete, and hence, to compute the optimum attacke, one needs to optimize the Holevo quantity with respect to a free parameter, e_y. We follow the optimization technique in [100] and conclude that the optimum attack occurs at $e_y = e_x$. Similar to the 6-state STR protocol, we assume an asymmetric version of the BB84 protocol and obtain

$$\begin{aligned} \bar{\chi}^{\text{BB84}}(X:E) &\leq \sum_{\lambda} p(\lambda)\, \bar{\chi}^{\text{BB84}}(\{\rho^{\lambda}_{ABT}, \mathbf{M}_{AB} \otimes \mathbf{M}^{\lambda}_{T}\}) \\ &= h(q_x) \end{aligned} \tag{5.77}$$

We consider again $Q = e_x^{a/b} = e_y^{a/b} = e_z^{a/b}$ for the numerical evaluation to obtain

$$\begin{aligned} \bar{R}^{\text{BB84}}_{\infty} &\geq \bar{I}(X:Y) - \bar{\chi}^{\text{BB84}}(\rho_{XE}) \\ &= 1 - 2\, h\big(2Q(1-Q)\big)\,. \end{aligned} \tag{5.78}$$

Figure 5.2 demonstrates the key rate of the BB84 STR protocol as a function of single-link error rate, Q, and compares it with the direct link BB84 protocol. The maximum tolerable single link

error rate drops from 11% to 5.8%.

5.8.3 Extension to a More General Attack

To obtain a numerical value for the key rate, we considered a special type of collective attacks, where the noisy quantum state of all users is written as a tensor product of two Bell diagonal states in Equation 5.68. The authors of [102] and [103] analyzed a more general type of collective attacks, where the noisy quantum state ρ_{ABT} is not necessarily in a product form, and instead, used the symmetry inherent in the QKD protocols to reduce the size of Γ_0 to a subset of Bell diagonal states. This simplifies the maximization of the Holevo quantity since the optimization runs over a smaller subset of free parameters.

Here is the summary of the key steps of the proof that is presented in [102] for the case of BB84 protocol:

1. The set of all density matrices that are compatible with the observed data, Γ_0, is extended to a larger space, $\Gamma_{e_{\vec{u}}}$, which is a set of all density matrices that are compatible with the basis dependent error rates.

2. It is shown that the Holevo quantity is invariant with respect to the local Pauli operators in each link, and therefore, the set of Pauli permuted states, $\Gamma_{\text{Pauli}} = \{\Pi_{\alpha\beta}\ \rho_{ATB}\ \Pi_{\alpha\beta}^{\dagger}\}$ results in the same error rate as $\Gamma_{e_{\vec{u}}}$. By definition the Pauli-permuting operator is

$$\Pi_{\alpha\beta} = \sigma_{\alpha}^{A} \otimes \sigma_{\beta}^{B} \otimes \sigma_{\alpha}^{T_a} \otimes \sigma_{\beta}^{T_b} \tag{5.79}$$

   where $\sigma_\alpha, \sigma_\beta \in \{\mathbb{1}, X, Y, Z\}$. Consequently, to maximize the Holevo quantity it is sufficient to optimize over the subset $\Gamma_{\text{Pauli}} \subset \Gamma_{e_{\vec{u}}}$.

3. The authors used the Pauli group permutation invariance property of the BB84 protocol and the concavity property of the Holevo quantity and showed that

$$\begin{aligned}
\max_{\Gamma_0}\ \chi(\{\rho_{ABT},\, \mathbf{M}_{ABT}\}) &\leq \sum_{\vec{u}} p(\vec{u})\ \max_{\Gamma_{e_{\vec{u}}}}\ \chi(\{\rho_{ABT}^{\vec{u}},\, \mathbf{M}_{AB}^{\vec{u}} \otimes \mathbf{M}_{T}^{\vec{u}}\}) \\
&\leq \sum_{\vec{u}} p(\vec{u})\ \max_{\Gamma_{\text{Pauli}}} \chi(\{\rho_{ABT}^{\text{Pauli}|\vec{u}},\, \mathbf{M}_{AB}^{\vec{u}} \otimes \mathbf{M}_{T}^{\vec{u}}\}) \\
&\leq \sum_{\vec{u}} p(\vec{u})\ \max_{\Gamma_{\text{Bell}}} \chi(\{\rho_{ABT}^{\text{Bell}|\vec{u}},\, \mathbf{M}_{AB}^{\vec{u}} \otimes \mathbf{M}_{T}^{\vec{u}}\})
\end{aligned} \tag{5.80}$$

where $\rho^{\text{Pauli}} = \Pi_{\alpha\beta}\ \rho\ \Pi^{\dagger}_{\alpha\beta}$, and

$$\rho^{\text{Bell}} := \frac{1}{16}\sum_{i=1}^{16}\rho_i^{\text{Pauli}} = \sum_{ij}\ \alpha_{ij}\ |\phi^i\rangle\langle\phi^i| \otimes |\phi^j\rangle\langle\phi^j|.$$

The author of [102] states that the same argument holds for the 6-state protocol.

Therefore, the particular noisy quantum state we considered in Equation 5.68 for numerical evaluation of the key rate, was a particular type of ρ_{Bell} with $\alpha_{ij} = \delta_i\eta_j$ that satisfies the constraint $\sum_i \delta_i = \sum_j \eta_j = 1$. By comparison between the result in Figure 5.2 with the numerical evaluation in [103], it is concluded that Equation 5.77 and Equation 5.76 provide a very good estimation of the optimum attack.

For the derivation of the above steps, we refer to [102] and [93], and for the numerical evaluation of the key rate in BB84 STR protocol, we refer to [103].

5.8.4 Insight on the security proof

In this section, we look at the parity announcement from another angle to get insight about the security proof.

For given λ, the T-node's adaptive measurements are given by POVM operators

$$\begin{aligned} \mathbf{T}^{\text{even}|\vec{u}} &= |00\rangle\langle 00| + |11\rangle\langle 11|_{u_1u_2}, \\ \mathbf{T}^{\text{odd}|\vec{u}} &= |01\rangle\langle 01| + |10\rangle\langle 10|_{u_1u_2}. \end{aligned} \tag{5.81}$$

Without loss of generality and for the sake of simplicity, we assume $u_1 = u_2 = Z$ and drop the index, u_1u_2. We then expand $\mathbf{T}^{\lambda}$ in terms of Bell states

$$\begin{aligned} \mathbf{T}^{\text{even}} &= |\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-|, \\ \mathbf{T}^{\text{odd}} &= |\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-|. \end{aligned} \tag{5.82}$$

This new expansion tells us that the two single qubit measurements followed by the parity announcement, λ, is theoretically equivalent to performing a joint measurement in Bell basis, which collapses the state of the two qubits to one of the Bell states, $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$, and then announcing the *parity* information (ϕ or ψ) publicly while keeping the phase information ($+$ or $-$) confidential. The key component of the STR protocol security proof is that the T-node is in the possession of some quantum information that is inaccessible to Eve. Precisely, there are two

measured quantum systems that is *shield* from Eve's access and a classical information that is *hidden* to her. Therefore, we consider a hypothetical experiment, where the *shield* quantum state is given to Eve but only once it is measured. A comparison between the actual STR protocol and this hypothetical experiment brings clarity to the security analysis.

Suppose Eve has access to both classical information of the T-node, parity and phase, but Alice and Bob only know the parity bit information. We rewrite the conditional quantum state ρ_{AB}^{λ} to obtain

$$\begin{aligned} \rho_{AB}^{\lambda} &= \frac{1}{p(\lambda)} Tr_T[(\mathbb{1}_{AB} \otimes \mathbf{T}^{\lambda})\, \rho_{ATB}], \\ &= \frac{1}{2}\,[\, p(+|\lambda)\, \rho_{AB}^{+|\lambda} + p(-|\lambda)\, \rho_{AB}^{-|\lambda}], \end{aligned} \tag{5.83}$$

where

$$\begin{aligned} \rho_{AB}^{\pm|\text{even}} &= \frac{1}{p(\pm|\text{even})}\, Tr_T[\mathbb{1}_{AB} \otimes |\phi^{\pm}\rangle\langle\phi^{\pm}|_T\, \rho_{ABT}], \\ \rho_{AB}^{\pm|\text{odd}} &= \frac{1}{p(\pm|\text{odd})}\, Tr_T[\mathbb{1}_{AB} \otimes |\psi^{\pm}\rangle\langle\psi^{\pm}|_T\, \rho_{ABT}]. \end{aligned} \tag{5.84}$$

Here, the probability, $p(+|\lambda)$, counts as the re-normalization factor. Note that we just rewrote the reduced density matrix of the legitimate users in a different way, and so, from Alice and Bob's perspective nothing has changed and the mutual information $I(X:Y|\lambda)$ in this hypothetical experiment is the same as before. However, the upper bound on Eve's information is slightly different. Eve has access to both classical bits about the *shield* quantum states: the parity bit, λ, and the phase bit $(\pm)$. Therefore, the reduced density matrix of Alice, Bob and Eve is updated to

$$\begin{aligned} \rho_{ABE}^{\lambda} &= p(+|\lambda)\, |\Psi^{+|\lambda}\rangle\langle\Psi^{+|\lambda}|_{ABE} \otimes |\lambda\rangle\langle\lambda|_C \otimes |+\rangle\langle+|_{\bar{E}}, \\ &+ p(-|\lambda)\, |\Psi^{-|\lambda}\rangle\langle\Psi^{-|\lambda}|_{ABE} \otimes |\lambda\rangle\langle\lambda|_C \otimes |-\rangle\langle-|_{\bar{E}}. \end{aligned} \tag{5.85}$$

Here, $|\Psi^{\pm|\lambda}\rangle$ is the purification of $\rho_{AB}^{\pm|\lambda}$ and the register $\bar{E}$ stores classical information that is only accessible to Eve. Intuitively, since extra information is given to Eve, Eve's knowledge either doesn't change or increases. Thus, the key rate can only decrease. Therefore, the lower bound on this hypothetical experiment is definitely a lower bound on the STR protocol.

We compute the key rate of the 6-state protocol for the above hypothetical experiment and obtain

$$\tilde{R}_{\text{Hypo.}}^{\text{6-state}} = 1 - h\,(2Q(1-Q)) - I_E\,(2Q(1-Q), 2Q(1-Q))\,.$$

This key rate has a negligible difference with the actual 6-state STR protocol as shown in Figure 5.2, The two key rates are indeed hardly distinguishable.

In BB84 protocol, the key rate is recalculated using Equation 5.85 and the result is

$$R_{\text{Hypo.}}^{\text{BB84}} = 1 - 2h\left(2Q(1-Q)\right).$$

Surprisingly, the two approaches yield identical key rates for the BB84 protocol. One may conclude that the proposed announcement strategy creates a classical correlation between the legitimate users' data as strong as the quantum correlation due to a two-qubit Bell measurement, and in this regard, a simplified trusted relay is similar to a quantum repeater.

5.9 Realistic considerations of STR-QKD

In standard security proof formalism of QKD, the key rate is typically derived under some assumptions that might not hold in practical implementation of QKD. One of those assumptions is that legitimate users generate infinite number of signals. Whereas, in realistic situation, there is a limit on the number of transmitted signals. Moreover, it is usually assumed that each pulse is a single-qubit signal, but, in practice, the weak coherent pulses are used which may contain multiple-photon signals. In this section, we account for these realistic situations and recalculate the key rate in each case.

5.9.1 Finite Size Effect:

In practical QKD, there is a time limit for the entire protocol, and so, a limit on the number of exchanged signals. Consequently, Alice, Bob and the T-node characterize the noisy quantum channel (or Eve's knowledge) based on their *"accessible information"* that might deviate from the ideal case. This deviation will affect the key rate and is considered in the following.

In the quantum phase of QKD, n number of signals are distributed, followed by the measurements. In the classical phase, particularly in the parameter estimation step, the legitimate users and the T-node sacrifice m bits of their data and obtain the statistics, $p_m(x,y,\vec{s})$, which deviates from the ideal probability distribution, $p_\infty(x,y,\vec{s})$, in asymptotic limit. According to the lemma 3 of [104], we define $\tilde{\Gamma}$ to be a set of all possible density matrices that are compatible with accessible information, p_m. Indeed,

$$\begin{aligned} \tilde{\Gamma} &:= \{\rho : \|p_\infty - p_m\| < \gamma\} \\ &\text{with} \\ \gamma(m,d) &:= \sqrt{\frac{2\ln(1/\varepsilon_{PE}) + d\ln(m+1))}{m}}, \end{aligned} \tag{5.86}$$

where ε_{PE} is the probability of failure in the PE step and d is the dimension of the signal. For single-qubits pulses, $d = 2$.

The *finite size effects* has been studied in [104] and [105], based on the theory developed by Rennato Renner in [95].The theory states that for limited number of exchanged signals, the key rate reduces to $R = \frac{l}{n} r$, where l is the length of the raw key and r is upper bounded by

$$r \leq S_\gamma(X|E) - \frac{(\text{leak}_{EC} + \Delta)}{l}. \tag{5.87}$$

Here, $S_\lambda(X|E) = \min_{\rho \in \tilde{\Gamma}} S(X|E)$ where $S(X|E)$ is the conditional von-Neumann entropy, and leak_{EC} is the amount of information that is leaked to Eve during the error correction step. The non-asymptotic effects appear as first, an extra term $\Delta = (2\log_2[1/2(\varepsilon - \varepsilon' - \varepsilon_{EC})]) + 5\sqrt{l \log_2[2/(\varepsilon' - \varepsilon_{PE})]}$, which depends on all the *security and concreteness* parameters [95], and second, an extra minimization over $\tilde{\Gamma}$. This minimization, in practice, results in replacing all error rates with $e \to e + \gamma$ to consider the worst-case scenario in the security analysis.

In the following, we take into account the finite size effects and derivation the key rate for both cases of the 6-state STR and the BB84 STR protocols.

6-state

Like before, we consider an asymmetric version of the 6-state protocol. With probability $p(u = Z) := p_z$, the basis Z is used for generating the key, and so, $l = np_z^2$ is the size of the raw data after the sifting step. In addition, the basis X and Y are used for the parameter estimation with the equal probabilities $p(u = X/Y) := p_x = (1 - p_z)/2$. Thus, the number of sacrificed bits in PE step is $m = np_x^2$. In the asymptotic limit, the conditional von-Neumann entropy is computed in a similar way to the computation of the Holevo quantity in Equation 5.76 and is

$$S(X|E) = (1 - \bar{e}_z)(1 - h\left(\frac{1 - (2\tilde{e}_x - \bar{e}_z)/2}{1 - \bar{e}_z}\right)$$

To account for the non-asymptotic limit, we replace $S(X|E) \to S_\gamma(X|E)$, which means to replace the basis dependent error rates $e_x^{(a/b)} \to e_x^{(a/b)} + \gamma(m, d = 2)$ in both links a/b. Similarly, $e_z^{(a/b)} \to e_z^{(a/b)} + \gamma(l, d = 2)$. To numerically evaluate the key rate, we assume $Q = e_y = e_x = e_y$ in both links and compute $H(X|Y) = \text{Leak}_{EC} = 1.2\ h(2Q(1 - Q))$. Given $S_\gamma(X|E)$ and Leak_{EC}, one should be able to compute the key rate using Equation 5.87. Note that $n, \varepsilon, \varepsilon_{EC}$ and Leak_{EC} are fixed by the protocol and one needs to do an optimization over the free parameters, $\varepsilon', \varepsilon_{PE}, l$ and m under the constraints $l + m < n$ and $\varepsilon > \varepsilon_{EC} > \varepsilon' > \varepsilon_{PE} > 0$. The numerical result is demonstrated in Figure 5.3 as a function of exchanged signals, n, for three different values of single-link error rate, Q.

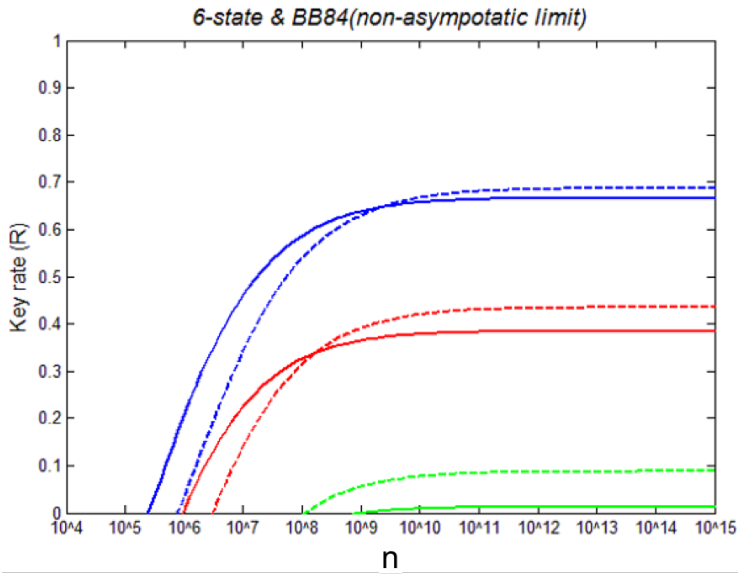

Figure 5.3: Key Rate as a Function of Total Number of Exchanged Signals, n: The solid lines belong to the BB84 protocol and the dashed lines belong to the 6-state protocol. We considered $\varepsilon = 10^{-9}$ and $\varepsilon_{EC} = 10^{-10}$ and the error rates of $Q = 0.5$ % (blue lines), 2% (red lines), and 5% (green lines).

BB84

Similarly, we consider an asymmetry version of the BB84 protocol, where the Z basis is used more frequently with probability p_z, and the X basis is used with probability $p_x = (1 - p_z)$. Thus, $l = np_z^2$ bits are used for key extraction, $m = np_x^2$ bits are used in PE step, and $2n\ p_x p_Z$ bits are discarded in the sifting step. The conditional von-Neumann entropy that accounts for the finite size effects is

$$S_\gamma(X|E) = 1 - h(\tilde{e}_x + 2\gamma). \tag{5.88}$$

Here, we replaced $e_x \to e_x + \gamma(m, d = 2)$ for both link a and b which leads to $\tilde{e}_x \to \tilde{e}_x + 2\gamma$. We optimized over the free parameters and obtained the key rate as a function of exchanged signals, n, and the result is plotted in Figure 5.3.

5.9.2 QKD with Decoy states

Another concern in practical QKD, which may threat the security, is the signal generators. In implementation of QKD with current technology, single-photon sources are highly attenuated lasers. However, laser pulses are described by coherent states where the probability of generating a pulse with n photons follows a Poisson distribution. This means, in addition to the single-photon pulses, there is a possibility of emitting multi-photon pulses which puts the security of the QKD protocols at risk of Photon Number Splitting (PNS) attack [106]. Nevertheless, a secure key can be generated if along with the actual pulses, the sender emits extra pulses with variant intensities- the so called *decoy state*- in order to estimate the lower bound on the number of detected single-photon pulses, [92, 107–110].

When sources generate coherent state pulses, there are different possibilities that may happen which are demonstrated in Figure 5.4. In order to guarantee the security of the STR-QKD protocols, we discard all events in which at least one of the sources (Alice's and/or Bob's) produces a multiple-photon pulse, because, Eve has full knowledge about the key due to PNS attack. If any of the sources produces a vacuum signal, neither Eve nor Alice and Bob can extract any information, thus, vacuum signals are also discarded. Therefore, it remains to consider that fraction of events that first, the sources generate single photon pulses, and second, the detectors at the T-node's laboratory *click*. The fraction of detected signals due to single-single photon pulses are denoted by F_{ss}, which are used for generating the secret key. The decoy-state techniques are used to estimate the lower bound on F_{ss}.

Suppose that Alice's source generates an x-photon pulse with probability $P_{\mu_a}(x) = e^{-\mu_a}\ \frac{\mu_a^x}{x!}$, where μ_a is the mean photon number. We denote the probability of event $\alpha \in \{\text{Detect}, \text{Not-Detected}\}$ occurring at the T_a-detector, with p_α^a. In addition, we define the *yield*, $Y_a(\alpha = \text{det}|x)$, as the probability of detecting an x-photon pulse at the T_a-detector. Because Eve is interfering with the Alice's and the T-node's communications, the yield $Y_a(\alpha|x)$ is unknown and depends on Eve's strategy. Given the above definitions, the fraction of pulses that are originated from Alice's source and ended in the T_a- detector is

$$f_x^a = \frac{P_{\mu_a}(x)\ Y_a(\alpha = \text{det}|x)}{p_{\text{det}}^a} \tag{5.89}$$

The error rate, e_x^a, arises from an x-photon pulse that is observed at the T_a-detector, and $x \in \{\text{Vaccume}(v), \text{Single}(s), \text{Multi}(m)\}$. In a similar manner, $P_{\mu_b}(y)$ denotes the probability of Bob's source generating a y-photon pulse, and f_y^b denotes the fraction of y-photon pulses that are detected at the T_b-detector.

Those useful events for key extraction are when both Alice's and Bob's source generates single photon pulses and both detectors click, i.e., $F_{ss} = f_s^a\ f_s^b$. Consequently, the key rate

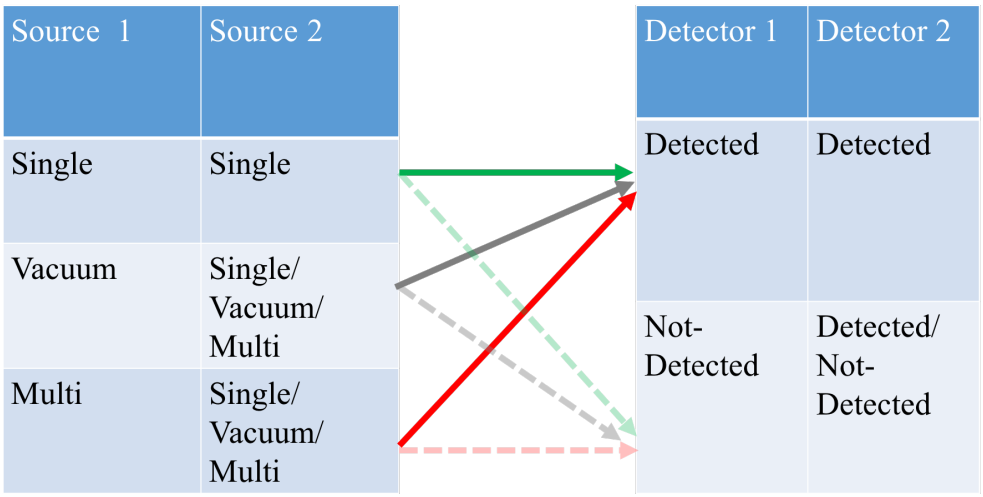

Figure 5.4: Two Multi Photon Sources and Possible Outcomes: The figure pictorially demonstrate possible combination of Vacuum pulses, Single photon pulses or Multi-photon pulses from two attenuated laser sources. The green arrows indicate those fraction of pulses that are useful for key extraction. The gray arrows are neutral pulses where neither Eve nor the legitimate users have any information. And, the red arrows are those fraction of events that Eve may have full knowledge about the secret key, and hence, are discarded.

reduces to $R_\infty = I(X:Y) - F_{ss}\,\chi(X:E)$[1]. Furthermore, we subtract those events that at least one of the sources generates a multi-photon pulse, because, Eve has full knowledge about the raw key data, in other words, $\chi(X:E) = 1$. The fraction of events with at least one multi-photon pulse is

$$\begin{aligned} F_m &\leq (1-f_s^a)\,f_s^b + f_s^a\,(1-f_s^b) + (1-f_s^a)\,(1-f_s^b) \\ &= (1-F_{ss}). \end{aligned} \tag{5.90}$$

Accordingly, the key rate is further reduced to

$$R_\infty = I(X:Y) - F_{ss}\,\chi(X:E) - F_m \tag{5.91}$$

To find the lower bound on key rate, we need to find a lower bound on the yield, $Y_{a/b}(\text{det}|s)$, and an upper bound on the errors due to single-photon pulses , $e_s^{a/b}$. The decoy state techniques have been extensively studied in literatures, such as [108] and [110], where coherent state pulses with

[1] Note that we indexed the key rate with ∞ to emphasize that the asymptotic limit of exchanged signals is considered.

variant intensities are used the users to estimate the lower bound on $f_s^{a/b}$ and the upper bound $e_s^{a/b}$ and we take it as a promise.

5.10 Summary

We proposed a variation of a quantum trusted relay network with three users, where the intermediate node uses a new announcement strategy to reassign the task of classical data processing to the end users. In simplified trusted relay protocol, the intermediate trusted node discloses the bit-wise parity information about each instances of its data, resulting in a direct correlation between the legitimate users' data, and therefore, substantial computation and communication resources at the trusted node is no longer required. The parity information provides enough classical correlation between Alice and Bob's data to perform Error Correction and Privacy Amplification by themselves. We provided the security proof for STR-QKD protocol in general and computed the key rate in particular cases of the 6-state protocol and the BB84 protocol. We numerically evaluated the key rate in the asymptotic limit and compared it with the single-link QKD. Furthermore, we considered the imperfections in practical QKD, such as finite size effects and multi-photon pulses.

Chapter 6

Conclusions and Future Works

Quantum Information Processing (QIP), with the ultimate goal of building a quantum device that has the potential of solving certain classical problems more efficient than a classical counterpart, has led to development of new theoretical tools such as the theory of open quantum systems and the theory of quantum error correction. The main contribution of this thesis sits at the border of QIP and Nuclear Magnetic Resonance (NMR) where the methods from the theory of open quantum systems are used to provide a more profound understanding of the spin noise signal in NMR and the experimental techniques from NMR are used to explore the noise protection ideas from the theory of quantum error correction.

Our work on the quantum model of spin noise brings clarity and accuracy in the description of the statistical fluctuation of a spin ensemble, known as spin noise. We have shown that the quantum mechanical nature of measuring an ensemble of spins results in the statistical fluctuations of the total spin magnetization that is independent of the external magnetic field but its amplitude scales with the square root of the number of spins. According to our model, correlations inherent in the spin noise have roots in the state disturbance introduced by the measurement and in the quantum evolution of the ensemble during the data acquisition. Our model analytically computes the statistical distribution and correlation function of the spin noise signal and the results unify the features of the spin noise in both limits of strong and weak measurement. This distinguishes our work from previous theoretical models. Our theory is applicable to any ensemble of quantum particles. In current work, the coil back action was taken into account in the state update rule but not during the free evolution time. Indeed, we modelled the evolution of the ensemble by a completely positive trace preserving (CPTP) map, which implies that the environment is memoryless and has no initial correlation with the spin system. In future work, one may consider non-CP maps in order to account for the memory effect of the environment that influences the dynamics of the spin ensemble.

Further, we investigated the concept of noiseless subsystem from the theory of quantum error correction in the NMR context. The work presented in Chapter 4 seeks for novel means of storing quantum information in the noise protected subspace of a group of identical spins. Our symmetry analysis of methyl groups' wavefunction shows that one can indirectly populate the noiseless subsystem of three identical protons through the electric dipole moment interaction of the molecule with the circularly polarized microwave field. For quantum computing purposes one may extend our work to initialize and control two logical qubits and test the scalability of this idea. In addition, we have shown that the noise protected qubit becomes an NMR observable through the dipolar relaxation processes of the methyl group and an external spin at high temperature. We analytically calculated the NMR spectrum and our theoretical results match reported experimental observations. Our approach makes no assumption about the spectral density of noise and solves the master equation only by relying on the symmetry properties of the spin operators in the interaction Hamiltonian. This approach might find application in other areas in NMR where the underlying physics of the relaxation mechanisms are of interest.

QIP has also had some commercial applications such as quantum key distribution (QKD) for secure communication. This thesis proposes a variation of QKD with trusted relay network in order to extend the range of key distribution to any arbitrary distance and overcome some of the practical challenges in the existing schemes. In our work, the intermediate node uses a new announcement strategy to create direct correlation between the legitimate users' data, leading to significant reduction in the classical resources required for data processing at the intermediate node. We showed that the two local measurements followed by the announcement is theoretically equivalent to a joint Bell measurement in a quantum repeater network but in our proposal no quantum memory is required. We analysed the efficiency of the key rate generated from our simplified trusted relay proposal for two cases of the BB84 and the 6-state protocols and account for finite source limit as well as imperfections in single photon signal generators. In future direction, one may extend our work to continuous variable QKD.

References

[1] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:6–7, 1982.

[2] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.Sci.Statist.Comput.*, 26:1484, 1997.

[3] M. S. Grinolds, and et al. Subnanometre resolution in three-dimensional magnetic resonance imaging of individual dark spins. *Nature Nanotechnology*, 7, 2014.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE*, page 175179, 1984.

[5] David Kielpinski, Chris Monroe, and David J Wineland. Architecture for a large-scale Ion-trap quantum computer. *Nature*, 417(6890):709711, 2002.

[6] A. Blais, R.-S. Huang, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf. Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation. *Phys. Rev. A*, 69:062320, 2004.

[7] D. G. Cory, M. D. Price, and T. F. Havel. Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing. *Physica D*, 261:120:82101, 1998.

[8] R. Annabestani, D. G. Cory and J. Emerson. Quantum model of spin noise. *JMR*, 252:94–102, 2015.

[9] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Experimental realization of Shors quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883887, 2001.

[10] Y. S. Weinstein, S. Lloyd, and D. G. Cory. Implementation of the quantum fourier transform. *Phys. Rev. Lett.*, 86:1889, 2001.

[11] L. J. Schulman, U. Vazirani. Scalable NMR quantum computation. 1998.

[12] D. G. Cory, and et al. NMR based quantum information processing: Achievements and prospects. 2000.

[13] C. Elliott. Building the quantum network. *New Journal of Physics*, 4(1):46, 2002.

[14] H. J. Briegel, W Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81(26):5932, 1998.

[15] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus. Security of quantum key Distribution using a simplified trusted relay. *Phys. Rev. A*, 91:012338, 2015.

[16] A. Einstein, B. Podolsky, and N. Rosen. Can quantum mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[17] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities. *Phys. Rev. Lett.*, 49:91, 1982.

[18] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time varying analyzers. *Phys. Rev. Lett.*, 49:1804, 1982.

[19] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, Cambridge, 1985.

[20] M. A. Nielsen, and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[21] H. Ollivier, and W. H. Zurek. Quantum discord: A measure of the quantumness of correlations. *Phys. Rev. Lett.*, 88, 2001.

[22] U. Haeberlen and J. S. Waugh. Coherent averaging effects in magnetic resonance. *Phys. Rev.*, 175:453, 1968.

[23] U. Haeberlen. High resolution NMR in solids. *Academic, New York*, 1976.

[24] W. Magnus. On the exponential solution of differential equations for a linear operator. *Communication on Pure and Applied Mathematics*, VII:649–673, 1954.

[25] M. M. Maricq. Long time limitations of the average Hamiltonian theory: A dressed-states viewpoint. *Advan. Mag. Res.*, pages 151–181, 1990.

[26] H. P. Breuer and F.Petruccione. *The theory of open quantum systems*. Oxford University Press, 2002.

[27] A.G. Redfield. The theory of relaxation processes. *JMR*, pages 1–32, 1965.

[28] A. Abragam. *The principles of nuclear magnetisim*. Clarendon Press, Oxford, 1962.

[29] R. R. Ernst, G. Bodenhausen and A. Wokaun. *The principles of nuclear magnetic resonance in one and two dimensions*. Clarendon Press, Oxford, 1985.

[30] J. Kowalewski and L. Maler. *Nuclear spin relaxation in liquids: Theory, experiments, and applications*. CRC press, 2006.

[31] A. J. Leggett and A. Garg. Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks? *Phy. Rev. Lett.*, 1985.

[32] A. E. Allahverdyana, R. Balianb and T. M. Nieuwenhuizen. Understanding quantum measurement from the solution of dynamical models. *Physics Reports*, pages 1–166, 2013.

[33] A. Peres. Neumark's theorem and quantum inseparability. *Foundation of Physics*, page 1441, 1990.

[34] J. Tropp. A quantum description of radiation damping and the free induction signal in magnetic resonance. *J. Chem. Phys*, 139:014105, 2013.

[35] C. P. Slichter. *Principles of magnetic resonance*. Springer, 1962.

[36] C. J. Wood. *Initialization and characterization of open quantum systems*. PhD Thesis, University of Waterloo, 2015.

[37] W. F. Stinespring. Positive functions on C^*-algebras. *Proc. Am. Math. Soc.*, page 211, 1955.

[38] K. Kraus. *States, effects and operations: Fundamental notions of quantum theory*. Lecture Notes in Physics. Springer, Berlin, 1983.

[39] E. J. Hinch. *Perturbation methods*. Cambridge University Press, 1991.

[40] M. D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, page 285, 1975.

[41] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, page 275, 1972.

[42] F. Bloch. Nuclear induction. *Phys. Rev.*, 70:460474, 1946.

[43] T. Sleator, E. L. Hahn, C. Hilbert and J. Clarke. Nuclear spin noise. *Phys. Rev. Lett*, 55:17421745, 1985-1987.

[44] M. A. McCoy, and R. R. Ernst. Nuclear spin noise at room temperature. *Chem. Phys. Lett*, 159:587593, 1989.

[45] M. Gueron and. J. L. Leroy. NMR of water protons. The detection of their nuclear-spin noise, and a simple determination of absolute probe sensitivity based on radiation damping. *J. Magn. Reson*, 85:209215, 1989.

[46] H. J. Mamin, R. Budakian, B.W. Chui, and D. Rugar. Detection and manipulation of statistical polarization in small spin ensembles. *Phys. Rev. Lett*, 91, 2003.

[47] C. L. Degen, M. Poggio, H. J. Mamin and D. Rugar. Role of spin noise in the detection of nanoscale ensembles of nuclear spins. *Phys. Rev. Lett*, 99:250601, 2007.

[48] C. A. Meriles, L. Jiang, G. Goldstein, J. S. Hodges, J. Maze, M. D. Lukin and P. Cappellaro. Imaging mesoscopic nuclear spin noise with a diamond magnetometer. *J. Chem. Phys*, 133:124105, 2010.

[49] J. M. Nichol, T. R. Naibert, E. R. Hemesath, L. J. Lauhon, and R. Budakian. Nanoscale fourier-transform magnetic resonance imaging. *Physical Review X*, 3, 2013.

[50] J. Hackmann, D. S. Smirnov, M. M. Glazov, F. B. Anders. Spin noise in a quantum dot ensemble: From a quantum mechanical to a semi-classical description. *Physica Status Solidi*, 251:12701275, 2014.

[51] N. Muller and A. Jerschow. Nuclear spin noise imaging. *PNAS*, 103:67906792, 2006.

[52] D. I. Houllt and N. S. Ginsberg. The quantum origin of the free induction decay signal and spin noise. *JMR*, 148:182199, 2001.

[53] M. Tavis and F. W. Cummings. Exact solution for an N-molecule radiation field Hamiltonian. *Phys. Rev*, 170:379, 1968.

[54] D. Poulin. Macroscopic observable. 2004.

[55] M. Nakahara and T. Ohmi. *Quantum computing from linear algebra to physical realization*. CRC Press, 2008.

[56] D. A. Lidar. Review of decoherence free subspaces, noiseless subsystems, and dynamical decoupling. *Advances in Chemical Physics*, 154, 2014.

[57] D. A. Lidar, K. B. Whaley. Decoherence-free subspaces and subsystems. 2003.

[58] A. Shabani and D. A. Lidar. Theory of initialization-free decoherence-free subspaces and subsystems. 2005.

[59] M. Carravetta and M. H. Levitt. Long lived nuclear spin states in high-field solution NMR. *J. AM. Chem. Soc.*, 126:6228–6229, 2004.

[60] M. Carravetta, O. G. Johannessen, and M. H. Levitt. Beyond the T_1 limit: Singlet nuclear spin states in low magnetic fields. *Phys. Rev. Lett.*, 92, 2004.

[61] K. Claytor and et al. Accessing long-lived disconnected spin1/2 eigenstates through Spins ¿ 1/2. *J. Am. Chem. Soc*, 136:1511815121, 2014.

[62] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84, 2000.

[63] L. Viola and et al. Experimental realization of noiseless subsystems for quantum information processing. *Science*, 293, 2001.

[64] L. Viola, E. Knill and R. Laflamme. Constructing qubits in physical systems. *J. Phys. A: Math. Gen.*, 34:70677079, 2001.

[65] D.D. Vvedensky. *Lecture note on group theory*. Imperial College London, 2001.

[66] year= 1996 publisher=Springer: New York T. Inui, Y. Tanabe, and Y. Onodera, title = Group theory and its applications in physics.

[67] M. Born and K. Huang. *Dynamical theory of crystal lattices*. Oxford University Press, New York, 1954.

[68] M. Borna and J.R. Oppenheimer. On the quantum theory of molecules. *Annalen der Physik*, 84:457–484, 1927.

[69] P. R. Bunker and P. Jensen. *Fundamentals of molecular symmetry*. Institute of Physics Publishing, 2005.

[70] P. R. Bunker. *Molecular symmetry and spectroscopy*. Academic Press, Inc (London), 1979.

[71] J. H. Freed. Quantum effects of methylgroup rotations in magnetic resonance: ESR splittings and linewidths. *J. Chem. Phys.*, 43:1710, 1965.

[72] P. S. Allen and Howard. On the modelling for a tunneling methyl group. *Chem. Phys. Lett.*, 6, 1970.

[73] S. Clough. Quantum tunnelling effects on nuclear magnetic resonance line width. *J. Phys. C: Solid St. Phys.*, 4, 1971.

[74] A.J. Horsewill. Quantum tunnelling aspects of methyl group rotation studied by NMR. *Progress in Nuclear Magnetic Resonance Spectroscopy*, 35:359389, 1999.

[75] R. M. Pitze. The barrier to internal rotation in ethane. *Am. Chem. Soc.*, 1983.

[76] V. Pophristic and L. Goodman. Hyperconjugation not steric repulsion leads to the staggered structure of ethane. *Nature*, 411, 2001.

[77] S. Jacobsen, U. Andresen, and H. Mäder. Microwave spectra of o-Fluorotoluene and its ^{13}C isotopic species: Methyl internal rotation and molecular structure. *Structural Chemistry*, 14, 2003.

[78] H. Rudolph, A. Z. Trinkaus and A. Naturforsch. *Naturforsch. A*, 23A:68, 1968.

[79] M. Icker and S. Berger. Unexpected multiple patterns incuded by the Haupt-effect. *JMR*, 219:1–3, 2012.

[80] M. Prager and A. Heidemann. Rotational tunneling and neutron spectroscopy: A compilation. *Chem. Rev*, 97:2933, 1997.

[81] K. Okuyama, N. Mikami and M. Ito. Internal rotation of the methyl group in the electronically excited state: o- and m-toluidine. *Laser Chem.*, 7:197–211, 1987.

[82] I.Kalkman,a C.Vu, M. Schmitt and W. L. Meerts. Structure and internal rotation in the S0 and S1 States of o-toluidine studied by high resolution UV spectroscopy. *Phys. Chem. Chem. Phys.*, 11:43114318, 2009.

[83] F. Bloch. ¨Uber die quantenmechanik der elektronen in kristallgittern. *Z. Phys.*, 52:555600, 1928.

[84] B. Meier and et al. Long-lived nuclear spin states in methyl groups and quantum-rotor-induced polarization. *J. Am. Chem. Soc.*, 135:1874618749, 2013.

[85] C.H. Townes and A. L. Schawlow. *Microwave spectroscopy*. Dover Publications, 1975.

[86] D. C. Harris and M. D. Bertolucci. *Symmetry and spectroscopy*. Oxford University Press, 1978.

[87] John David Jackson. *Classical electrodynamics*. Wiley, 1962.

[88] G. B. Matson. Methyl NMR relaxation due to dipolar interactions. *J. Chem. Phys.*, 65:4147, 1976.

[89] B. Blicharska. Theoretical description of the methyl group relaxation in liquids. *Physica*, 147A:601–626, 1988.

[90] A. Shamir R.L. Rivest and L. Adlema. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[91] H. Riedmatte N.Sangouar, C. Simon and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:3380, 2011.

[92] A. MacDonald and et al. How to implement decoy state quantum key distribution for a satellite uplink with 50-db channel loss. *Phys. Rev. Lett.*, 2011.

[93] A. Ferenczi. *Security proof methods for quantum key distribution protocols*. PhD Thesis, University of Waterloo, 2013.

[94] A. Ferenczi and N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A.*, 85:052310, 2012.

[95] R. Renner. *Security of quantum ley distribution*. PhD Thesis,ETH Zurich, 2005.

[96] R. Konig, M. Christandl and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, 2009.

[97] R. Renner, N. Gisin, and B. Kraus. Information theoretic security proof for quantum key distribution. *Phys. Rev. A*, 72:012332, 2005.

[98] H.-K. Lo, H. Chau, and M. Ardehali. Efficient quantum key distribution scheme and proof of its unconditional security. *J. Cryptology*, 18:133, 2005.

[99] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441, 2000.

[100] V. Scarani and et al. A framework for practical quantum cryptography. *Rev. Mod. Phys.*, 81:1301, 2009.

[101] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution psrotocol. *Phys. Rev. Lett.*, 85:441444, 2000.

[102] W. S. Stacey. *The Security of Simplified Trusted Relays*. MSc Thesis, University of Waterloo, 2014.

[103] W. S. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus. Security of quantum key distribution using a simplified trusted relay. *Phys. Rev. A.*, 91:012338, 2015.

[104] V. Scarani and R. Renner. Quantum cryptography with finite resources. *Phys. Rev. Lett*, 100:200501, 2008.

[105] V. Scarani and R. Renner. Security bounds for quantum cryptography with finite resources. 2008.

[106] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, 2004.

[107] H. Inamori, N. Lütfaus, and D. Mayers. Unconditional security of practical quantum key distribution. *The European Physical Journal*, 41(3):599627, 2007.

[108] H.K. Lo, X. Ma, and K. Chen. Decoy dtate quantum key distribution. *Phys. Rev. Lett.*, 94:230504, 2005.

[109] A. Acin, N. Gisin, and V. Scarani. Coherent pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks. *Phys. Rev. A.*, 69:012309, 2004.

[110] D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.*, 4(5):325, 2004.

Appendix A

Rate Equation

In the main text, we solved the rate equations for short evolution time, $t = \delta t$. To compute the change of population of the x^{th} energy level during t_0 and $t_0 + \delta t$, it is required to know the population difference between the x^{th} level and all other energy levels y at time t_0 which are allowed due to the DQ^{λ} and ZQ^{λ} terms of DD coupling. For the first step, when $t_0 = 0$, the calculation of population difference between allowed transitions yields Equation 4.78 when the test spin is unpolarized, and results in Equation 4.84 when the est spin has a polarization $\alpha \neq 0$. In this appendix, we move one step forward and compute the change of population of the x^{th} level during $t = \delta t$ and $t = 2\delta t$. This requires the calculation of population difference between the allowed transitions, x and y, at an earlier time, $t_0 = \delta t$. This is computed by

$$[x]_{\delta t} - [y]_{\delta t} = [x]_0 - [y]_0 + \Delta[x]_1 - \Delta[y]_1. \tag{A.1}$$

The first two terms, $[x]_0 - [y]_0$ are already calculated in Equation 4.84. To compute the second two terms, we assume $\alpha = 0$, for simplicity, and use the result in Equation 4.80. We start from $m = \pm\frac{3}{2}$ and obtain

$$\begin{aligned}
\Delta[A, \frac{3}{2}, \uparrow]_1 - \Delta[E_{\pm}, \frac{1}{2}, \downarrow]_1 &= -\delta t\ (a_0 + a_{\pm}) \\
\Delta[A, \frac{3}{2}, \downarrow]_1 - \Delta[E_{\pm}, \frac{1}{2}, \uparrow]_1 &= -\delta t\ (b_0 + b_{\mp}) \\
\Delta[A, -\frac{3}{2}, \downarrow]_1 - \Delta[E_{\pm}, -\frac{1}{2}, \uparrow]_1 &= -\delta t\ (a_0 + a_{\mp})^{\beta \to -\beta} \\
\Delta[A, -\frac{3}{2}, \uparrow]_1 - \Delta[E_{\pm}, -\frac{1}{2}, \downarrow]_1 &= -\delta t\ (b_0 + b_{\mp})^{\beta \to -\beta}
\end{aligned} \tag{A.2}$$

in which a_0, b_0, $a_\pm$ $b_\pm$ are constants and the subscript $\beta \to -\beta$ means that in the definition of these constants, β is replaced with $-\beta$. Those constants are explicitly

$$
\begin{aligned}
a_0 &= \frac{\gamma}{4}\,(J_2^{E_+} + J_2^{E_-} + \frac{J_0^{E_+} + J_0^{E_-}}{18}) + \beta\,\frac{(1-\gamma)}{8}\,(J_2^{E_+} - J_2^{E_-}) \\
b_0 &= \frac{\gamma}{4}\,(\frac{J_0^{E_+} + J_0^{E_-}}{6} + \frac{J_2^{E_+} + J_2^{E_-}}{3}) + \beta\,\frac{(1-\gamma)}{8}\,(J_2^{E_+} - J_2^{E_-}) \\
a_\pm &= \frac{\gamma}{4}\,(J_2^{E_\pm} - \frac{J_0^{E_\pm}}{18}) \pm \beta\,\frac{(1-\gamma)}{8}\,(\frac{J_0^{E_\pm}}{9} + \frac{J_0^{E_\mp}}{18}) \\
b_\pm &= \frac{\gamma}{4}\,(\frac{J_0^{E_\pm}}{6} - \frac{J_2^{E_\pm}}{3}) \pm \beta\,\frac{(1-\gamma)}{8}\,(\frac{2J_2^{E_\pm}}{3} + \frac{J_2^{E_\mp}}{3})
\end{aligned}
\tag{A.3}
$$

The expressions in Equation A.2 gives the population difference between allowed transitions at time $t_0 = \delta t$. Thus, we substitute Equation A.2 into the rate equation, Equation 4.75, in order to calculate $\Delta[x]_2$ and the result is

$$
\begin{aligned}
\Delta[A, \frac{3}{2}, \uparrow]_2 &= \Delta[A, \frac{3}{2}, \uparrow]_1 + \delta t^2\,((a_0 + a_+)\,J_2^{E_+} + (a_0 + a_-)\,J_2^{E_-}) \qquad \text{(A.4)} \\
\Delta[A, \frac{3}{2}, \downarrow]_2 &= \Delta[A, \frac{3}{2}, \downarrow]_1 + \frac{\delta t^2}{6}\,((b_0 + b_+)\,J_0^{E_+} + (b_0 + b_-)\,J_0^{E_-}) \qquad \text{(A.5)}
\end{aligned}
$$

(A.6)

$$
\begin{aligned}
\Delta[A, -\frac{3}{2}, \uparrow]_2 &= \Delta[A, -\frac{3}{2}, \uparrow]_1 + \frac{\delta t^2}{6}\,((b_0 + b_-)\,J_0^{E_-} + (b_0 + b_+)\,J_0^{E_+})^{\beta \to -\beta} \\
\Delta[A, -\frac{3}{2}, \downarrow]_2 &= \Delta[A, -\frac{3}{2}, \downarrow]_1 + \delta t^2\,((a_0 + a_-)\,J_2^{E_-} + (a_0 + a_+)\,J_2^{E_+})^{\beta \to -\beta}
\end{aligned}
$$

Then, to compute the NMR signal on the test spin channel condition on the collective spin magnetization $m = \pm\frac{3}{2}$, we subtract the above expressions from each other and in the calculation, we encounter terms like this

$$
(a_0 + a_+)J_2^{E_+} - (b_0 + b_+)\frac{1}{6}J_0^{E_+} = \frac{\gamma}{4}\,A + \beta\,\frac{1-\gamma}{8}\,B
$$

which is written in such a way that A contains all terms with $\frac{\gamma}{4}$ dependency and B contains all terms with $\beta\frac{1-\gamma}{8}$. This helps us to analyse the feature of the NMR peaks regardless of the explicit form of the spectral density of noise. Intuitively, if $\beta = 0$, the NMR signal from $\pm m$ have the same amplitude but with opposite sign. This is because the counter part of $|A, +\frac{3}{2}, \uparrow\rangle$ is $|A, -\frac{3}{2}, \downarrow\rangle$ where both are involved in DQ transition and the counterpart of $|A, +\frac{3}{2}, \downarrow\rangle$ is $|A, -\frac{3}{2}, \uparrow\rangle$

where both are involved in ZQ transition. Thus, the contribution from the $\frac{\gamma}{4}$ dependent terms results in an anti-phase signal from $m = \pm\frac{3}{2}$ peaks. In contrast, the contribution from the β dependent terms results in an in-phase signal from $m = \pm\frac{3}{2}$ peaks, because, $m = -\frac{3}{2}$ picks an additional minus when $\beta \to -\beta$. Therefore, given the expressions in Equation A.4 and the first order calculation that was given in the main text in Equation 4.83, the second order anticipated NMR signal for evolution time, $t = 2\ \delta t$ is

$$\langle \Pi^{\pm\frac{3}{2}} \otimes I_z \rangle_{2\delta t} \quad = \quad \langle \Pi^{\pm\frac{3}{2}} \otimes I_z \rangle_{\delta t} + \frac{\delta t^2}{8} \{\pm\gamma A + \beta \frac{(1-\gamma)}{2} B\} \tag{A.7}$$

The same logic holds for $m = \pm\frac{1}{2}$ NMR peaks and similar feature is obtained,

$$\langle \Pi^{\pm\frac{1}{2}} \otimes I_z \rangle_{2\delta t} \quad = \quad \langle \Pi^{\pm\frac{1}{2}} \otimes I_z \rangle_{\delta t} + \frac{\delta t^2}{8} \{\pm\gamma A' + \beta \frac{(1-\gamma)}{2} B'\} \tag{A.8}$$

It is important to note that in contrast to the calculated NMR signals for $t = \delta t$, here at $t = 2\delta t$, the NMR peaks of $m = \pm\frac{1}{2}$ do not have the same amplitude as that of $m = \pm\frac{3}{2}$. This has root in the fact that at $t = \delta t$, all energy levels within each symmetry subspace are not equally populated any more, leading to $A \neq A'$ and $B \neq B'$.

To conclude, the solution of the rate equations for the second step, $t = 2\delta t$, has similar features to that of Equation 4.80, and therefore, all arguments in the main text regarding the phase and amplitude of the NMR peaks which were concluded for short evolution $t = \delta t$, can be generalize to any time evolution by inductive reasoning.