Exploring quantum foundations by NMR: Quantum correlations and measurements

A thesis

Submitted in partial fulfillment of the requirements of the degree of

Doctor of Philosophy

by

C S Sudheer Kumar

Registration ID-20133285

NMR Research Center and Department of Physics

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH

PUNE-411008, India

March 2021

Certificate

Certified that the work incorporated in the thesis entitled **"Exploring quantum foundations by NMR: Quantum correlations and measurements"** submitted by **C S Sudheer Kumar** was carried out by the candidate, under my supervision. The work presented here or any part of it has not been included in any other thesis submitted previously for the award of any degree or diploma from any other university or institution.

Date: 24-March-2021
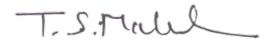
Prof. T.S. Mahesh

(Supervisor)

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Date: 24-March-2021

C S Sudheer Kumar
(Registration ID: 20133285)

"There is no law other than the law that there is no law"-John Archibald Wheeler (Science and ultimate reality, Cambridge university press (2005)).

"Goal of life is not to follow the laws of nature, but to break them and go beyond"-Swami Vivekananda (Complete works).

"Dissatisfaction with the first view of things is the mother of all metaphysics (physics). While common sense accepts the surface phenomenon as real, reflection asks whether the first view is to be regarded as the final one."-S Radhakrishnan (Indian Philosophy, Oxford university press (2010)).

Dedicated to the people of India

Acknowledgments

Universe is a self excited circuit. Evolving from big bang, it gives rise to observer-participancy, and looks backwards towards itself-J A Wheeler [WZ83]. Violation of Bell's inequality clearly shows that separation in space and time (Einstein separability) is not a fundamental fact of nature. This is further justified by "Ekam sat wipra bahuda vadanti (that one, second-less supreme reality is manifesting itself as many)."-Upanishads. Nature is like a mirror through which the one supreme reality is trying to look at its own face. Hence acknowledgment does not make sense from the point of view of the absolute reality. As long as we are maintaining classical notion of separate individual identities for the sake of worldly affairs, it may make sense. Hence for practical purposes I would like to acknowledge.

It is a pleasure to thank my supervisor Prof T S Mahesh for the wonderful guidance, freedom, support, and the encouragement he has given me throughout. My special thanks to him for initiating the project on quantum state discrimination.

I am very much grateful to my collaborators Prof. T S Mahesh, Dr. Hemant Katiyar, Dr. Abhishek Shukla, Prof. Anup Biswas, Prof. Ujjwal Sen, and Prof. Aditi Sen(De) for all the insightful discussions, support, and encouragement they have given me throughout.

My special thanks to Prof Deepak Dhar, and Prof M S Santhanam for the very insightful discussions, critical comments, and suggestions they have given me.

I express my sincere thankfulness to my lab members Swathi Hegde, Anjusha V. S., Deepak Khurana, V. R. Krithika, Soham Pal, Govind Unnikrishnan, Gaurav Bhole, and Dr. Rupak Bhattacharya for all the very useful discussions.

List of publications

(1) NMR investigation of contextuality in a quantum harmonic oscillator via pseudospin mapping.

Hemant Katiyar, C.S. Sudheer Kumar, and T.S. Mahesh.

Europhysics Letters, 113, 20003 (2016) [KKM16]. arXiv:1503.05883 [quant-ph].

(2) Discriminating between Luders and von Neumann measuring devices: An NMR investigation.

C. S. Sudheer Kumar, Abhishek Shukla, and T. S. Mahesh.

Physics Letters A, 380, 3612 (2016) [KSM16]. arXiv:1607.05723 [quant-ph].

(3) Ancilla-induced amplification of quantum Fisher information.

C. S. Sudheer Kumar, and T. S. Mahesh.

The European Physical Journal Plus (2018) 133: 460 [SKM18]. arXiv:1801.01396 [quant-ph].

(4) Violation of space-time Bell-CHSH inequality beyond Tsirelson bound and quantum cryptography.

C. S. Sudheer Kumar.

Pramana-J. Phys. (2019) 93:67 [SK19]. arXiv:1702.05479 [quant-ph].

(5) Frequentist-approach inspired theory of quantum random phenomena predicts signaling.

C. S. Sudheer Kumar, Anup Biswas, Aditi Sen(De), and Ujjwal Sen.

arXiv:1903.12096v2 [quant-ph] [SKBSS20].

(6) Quantum Correlations in NMR systems.

T. S. Mahesh, C. S. Sudheer Kumar, and Udaysinh T. Bhosale.
Invited book chapter (Springer)-ISBN 978-3-319-53410-7 [MSKB17]. arXiv:1608.06579 [quant-ph].

(7) How many runs ensure quantum fidelity in teleportation experiment?
C. S. Sudheer Kumar, and Ujjwal Sen.
arXiv:2004.14816v1 [quant-ph].

(8) Star-topology Registers: NMR and Quantum Information Perspectives.
T S Mahesh, Deepak Khurana, Krithika V R, Sreejith G J, and C S Sudheer Kumar.
arXiv:2102.05203 [quant-ph] [MKR$^+$21].

(9) Ancilla assisted measurements on quantum ensembles: General protocols and applications in NMR quantum information processing.
T. S. Mahesh, Abhishek Shukla, Swathi S. Hegde, C. S. Sudheer Kumar, Hemant Katiyar, Sharad Joshi, K. R. Koteswara Rao.
Current Science, 109, 1987 (2015) [MSH$^+$15]. arXiv:1509.04506 [quant-ph].

ABSTRACT

Research into quantum information and quantum computation has raised many fundamental questions. To make progress, a critical understanding of the fundamental aspects has become inevitable. Here we investigate, both experimentally and theoretically, some of the fundamental aspects of quantum mechanics viz., quantum contextuality, quantum measurement, quantum Fisher information, no-signaling principle, and quantum nonlocality.

Using a three qubit NMR register, we show that, quantum harmonic oscillator states exhibits quantum contextuality (i.e., no reality before measurement; in other words, we cannot assign values to observables even before measurement; measurement creates reality). Using a four qubit NMR register, we show that, NMR spectrometer is a Luders measuring device (which preserves superposition in the degenerate subspace corresponding to a degenerate observable being measured). Using a four qubit NMR star topology register (i.e., one central target qubit surrounded by three ancillary qubits), we show that, ancillary qubits pre-correlated with central target qubit, can amplify quantum Fisher information corresponding to the central target qubit (i.e., increases precision in unknown parameter estimation corresponding to the central target qubit).

Density matrix description is based on Kolmogorov's modern axiomatic probability measure theory of quantum random phenomena. However, in Kolmogorov's schema, *a priori* assumption of a constant value for the probability of a single random event is a purely mathematical quantity which is not motivated by experiment. Consequently, motivated by what we actually observe in experiments, we propose an alternative mathematical model wherein *a priori* probability measure is dropped completely and instead *a posteriori* limit-supremum of relative frequency is considered. We call the resulting theoretical model as the frequentist-inspired quantum mechanics wherein we consider the unknown

quantum states path by path. Then we show that within the frequentist-inspired quantum mechanics, physically different ensembles described by the same density matrix are distinguishable via content dependent fluctuations.

Finally we show that, it is possible to violate Bell's inequality beyond Tsirelson bound by introducing context dependent unitary evolutions. Correct context dependency can be achieved by either post-selection or signaling. This leads to a more efficient quantum key distribution protocol.

Table of Contents

xiv

List of Figures

List of Tables

CHAPTER 1

Introduction

1.0.1 Why research into quantum foundations?

Research into quantum information and quantum computation has raised many fundamental questions viz., is it possible to copy an unknown quantum state? How is the superposition broken when we move to the classical domain from the quantum domain? Is the density matrix description complete i.e., does it carry all the information which an observer has about a given quantum system/ensemble? Even though entangled particles can somehow communicate superluminally (see [Pop14] in this regard; also the Refs. [STZG00, SBB$^+$08] puts a lower bound of $2 \times 10^4 c$ on the speed where c is the speed of light in vacuum), why cannot we use it for superluminal communication, what prohibits us from doing so? Can we exploit quantum correlations to go beyond shot-noise limit in estimating an unknown parameter? Why does an observer plays a dynamical role in the quantum world (e.g., outcomes of measurement depends on the way he measures i.e., quantum contextuality; Wheeler's delayed choice experiment etc.) which is unlike in classical world? etc. Further we get access to new resources present in the nature, only when we question the domain of validity of so called well established facts/laws. Attitude of 'shut up and do calculation' cannot take us much forward. 'There is no law other than the law that there is no law' -J A Wheeler [bJDBDJ05]. 'Law without law'-J A Wheeler [WZ83, Sto15]. This is evident from the history of physics. When we questioned the domain of validity of Newtonian and classical mechanics, we were able to explore relativistic and quantum domains, thereby we got access to new resources.

Measurement precision: QFI (Chapter-4)

Reality before ? (Chapter-2)

Measuring device: Luders/ von Neumann? (Chapter-3)

Can post-selection lead to much stronger violation of Bell inequality ? (Chapter-6)

Is density matrix description complete? (Chapter-5)
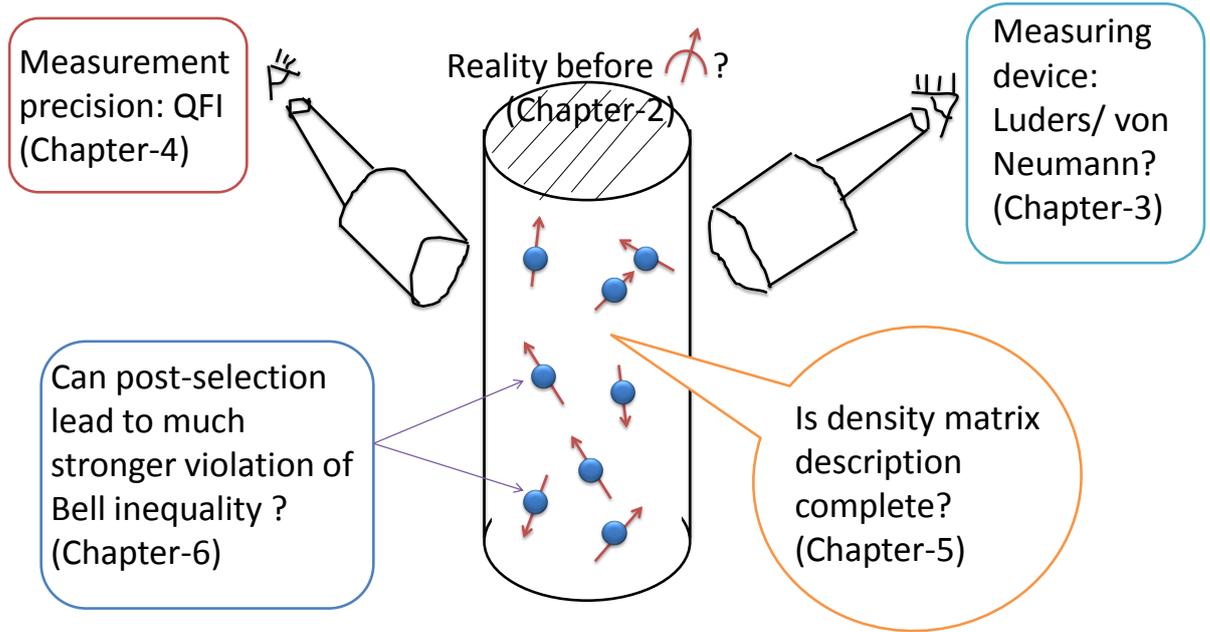
In our opinion, fundamental aspects of quantum mechanics is the most fundamental physical theory, currently. Nowhere else in physics, observer plays such a dynamical role: Wheeler's delayed choice experiment (Wheeler's 'participatory universe', 'it from bit') [WZ83, Sto15], there is no reality before measurement but observer creates reality which in turn depends on the way he measures (quantum contextuality [Per90]), consciousness induced collapse of the state vector [vN55, WZ83, Hom97, Lal04]. Importance of the role of observer can be further justified by Penrose's assertion (which is based on Goedel's incompleteness theorem) that human mind has non-algorithmic/non-computational/non-mechanistic powers in its nature/functioning [Pen06]. Further quantum nonlocality implies that separation in space and time is only a classical notion but not a fundamental one: Two entangled particles can somehow communicate instantaneously/superluminally [Pop14] (Refs. [STZG00, SBB$^+$08] puts a lower bound at $2 \times 10^4 c$ on the speed); Observer can affect, by traveling backward in time, the past history of a photon (Wheeler's delayed choice experiment on astronomical scale: Wheeler's participatory universe) [WZ83, Sto15]. By researching into quantum foundations, we

may get access to new resources like nonlinear evolution, signaling, cloning etc., and also it may bridge the gap in our understanding of the connection between mind and matter, and how they affect each other [Pen06].

In this thesis, we explore the foundations of quantum mechanics, both experimentally and theoretically. We use nuclear magnetic resonance (NMR) architecture as our experimental test bed to investigate quantum contextuality, Luders and von Neumann measurements, and exploiting quantum correlation to achieve better precision in quantum metrological tasks. Theoretically we investigate, distinguishing between two differently prepared and physically different ensembles described by the same density matrix, and violation of Bell's inequality beyond Tsirelson bound via post-selection. In the following we briefly introduce the basic concepts of quantum information and NMR.

1.1 Basics of quantum information and quantum computing

1.1.1 State vector description without a probability measure

The basic building block of classical information is bit, which can take only two values viz., 0 or 1. Whereas the basic building block of quantum information is qubit (quantum bit), which can exist not only in the state $|0\rangle = [1 \ 0]^{\mathrm{T}}$ (T stands for matrix transpose) or $|1\rangle = [0 \ 1]^{\mathrm{T}}$, but it can also exist in an arbitrary superposition of $|0\rangle$ and $|1\rangle$ i.e.,

$$|\theta, \phi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle \tag{1.1}$$

which is the Bloch sphere representation (SU(2) to SO(3) homomorphism [AW01]) [NC10]. $|\theta, \phi\rangle$ belongs to the Hilbert space which is a linear complex vector space

spanned by state vectors [CTDL05, Aud07]. This quantum superposition is the new resource which can be used to speed up computations (Shor's prime factorization algorithm [NC10, PMA$^+$19]), speed up unsorted data search (Grover's search algorithm [NC10]), teleport a quantum state (via entanglement which is also nothing but superposition in an higher dimensional Hilbert space) [NC10], unconditionally secure cryptography [Paw10] etc. Linear nature of quantum mechanical operators (unitary evolution operator) is the one which makes possible the superposition of states to exist. But this very linear nature prohibits cloning/copying an unknown quantum state [WZ82].

Standard text book quantum mechanics is based on existence of a state vector corresponding to a given physical system and *a priori* assumption of a probability measure to describe quantum random phenomena. However it is possible to make predictions (stochastically but not deterministically) even without assuming *a priori* a probability measure. This approach is known as pathwise approach [Son06] or individualist approach [GLTZ19] or frequentist-inspired approach [SKBSS20]. In fact state vector with a probability measure is equivalent to/nothing but density matrix description which is described in the next section.

1.1.2   Density matrix description

We cannot predict deterministically the outcome of measuring, say σ_z (Pauli-z observable) on $|\theta, \phi\rangle$. The non-linear collapse dynamics (i.e., quantum measurement problem) is not yet understood [Hom97]. This results in quantum randomness. Mathematical model of random phenomena used in all standard quantum mechanics books is A N Kolmogorov's modern axiomatic, probability measure theoretic approach (see Appendix 8.1). It assumes *a priori* existence of a probability measure i.e., it assigns *a priori* a real number between 0 and 1 for the probability of a single random event which is a subjective measure of how likely the event occurs. E.g., it assigns probability 1/2 to a

single outcome $+1$ in a measurement of σ_z on $(|0\rangle + |1\rangle)/\sqrt{2}$ where $|0\rangle, |1\rangle$ are eigenkets of σ_z with eigenvalue $+1, -1$ respectively (it is based on intuitive/subjective notion of "equally likely" events). Important point to be noted here is, it is assigning *a priori* a constant value for the probability of a single random event (no ensemble here) i.e., it predicts probabilistically (but not deterministically) the outcome of a single random event. Probability measure is a purely mathematical assumption which is not based on experiment (i.e., relative frequency). However strong law of large numbers tries to connect, in some sense, the theoretical probability with experiment [Gut05, Ros10].

According to Born's statistical/probabilistic interpretation of $|\theta, \phi\rangle$ [Gri95] (which uses Kolmogorov's model), upon measuring σ_z on $|\theta, \phi\rangle$, the state vector collapses to $|0\rangle(|1\rangle)$ with probability $\cos^2(\theta/2)(\sin^2(\theta/2))$. This in turn gives rise to the density matrix description, according to which the state of a single qubit is described by the density matrix

$$\rho = |\theta, \phi\rangle\langle\theta, \phi|. \tag{1.2}$$

Note that in $|\theta, \phi\rangle$ there are no probabilities and hence quantum randomness has not yet come into picture. Whereas in ρ, diagonal elements are probabilities of measurement outcomes, and off-diagonal elements are coherences (a measure of superposition property), and hence quantum randomness/probabilistic nature of measurement outcomes has been built into it. Hence the theory of random phenomena which we have used (i.e., Kolmogorov's model) plays a crucial role in judging the completeness/incompleteness of density matrix description. This observation is relevant in the light of the following works [PSCWH00, LZJ$^+$06, Pop18, SKBSS20, GLTZ19], p16 of [Aud07]. Now we can

5

generalize the concept of density matrix to mixtures of many quantum states as follows

$$\rho' = \sum_j p_j |\theta_j, \phi_j\rangle\langle\theta_j, \phi_j| \qquad (1.3)$$

where p_j is the probability/weight corresponding to $|\theta_j, \phi_j\rangle$, and $\sum_j p_j = 1$ [vN55] (also see Appendix 8.2 in this regard). Note that even mixtures of quantum states can be described by state vectors [LZJ$^+$06, SKBSS20]. Density matrices belong to Liouville space which is a linear complex vector space whose elements are linear operators acting on a Hilbert space. These linear operators satisfy the axioms of a linear vector space like existence of basis, scalar/inner product, norm, incoherent superposition (because $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2$ exhibits no interference) etc. [Aud07]. The dyadic decomposition of an operator in Liouville space is the following [Aud07]:

$$A = \sum_{i,j} A_{ij} |i\rangle\langle j| \qquad (1.4)$$

where $A_{ij} = \langle i|A|j\rangle$, and $\{|i\rangle\langle j|\}$ is a basis in Liouville space. As A_{ij} are complex numbers in general, Liouville space is also complex. It is important to note that, according to the basic postulate of quantum mechanics, state of any physical system (including mixtures of many quantum states) is described by a set of state vectors or a single state vector/ket with unknown parameters in it (but not density matrix) belonging to the Hilbert space [CTDL05, Sha08, LZJ$^+$06]. E.g., in quantum teleportation, nocloning theorem, BB84 etc. (see Sec. 5.4 for more details).

1.1.3 No unique decomposition of a mixed density matrix

An interesting and controversial consequence of density matrix description is the following. A given density matrix (which is mixed i.e., $\mathrm{Tr}(\rho'^2) < 1$ where $\mathrm{Tr}(.)$ is the trace

operator) can be decomposed in infinitely many ways. E.g.,

$$\begin{pmatrix} 0.7 & 0 \\ 0 & 0.3 \end{pmatrix} = 0.7 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 0.3 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= 0.4 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 0.3 \begin{pmatrix} 0.64 & 0.48 \\ 0.48 & 0.36 \end{pmatrix} + 0.3 \begin{pmatrix} 0.36 & -0.48 \\ -0.48 & 0.64 \end{pmatrix} \qquad (1.5)$$

where, in the second line, middle density matrix is the outer product of the state $[0.8 \quad 0.6]^{\mathrm{T}}$ and the last density matrix is the outer product of the state $[0.6 \quad -0.8]^{\mathrm{T}}$ [Per95]. Another simple example is the following. $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2 = (|+\rangle\langle +| + |-\rangle\langle -|)/2 = \mathbb{1}_2$ where $|\pm\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $\mathbb{1}_n$ is the $n \times n$ identity matrix. Consequently, according to density matrix description, one cannot distinguish between two different ensemble/single quantum state preparation procedures, both of which are described by the same density matrix. This in turn prohibits superluminal communication via entangled qubits. We will take up this issue in chapter 5.

As qubits are distinguishable (by their spatial location or chemical shift in NMR etc.), we can ignore symmetrizing or anti-symmetrizing the total state vector describing the state of the physical system (bunch of qubits) under consideration [Sha08].

There are many ways of quantifying quantum information viz., quantum Fisher information (metrology) [TA14], von Neumann entropy as a measure of quantum information (entanglement measure) [Aud07], Wigner-Yanase skew information [TA14], quantum mutual information (quantum discord measure) [MSKB17, KLKW18] etc. All these are interrelated i.e., we can usually express one in terms of the other for a given quantum system [Fri99, KLKW18].
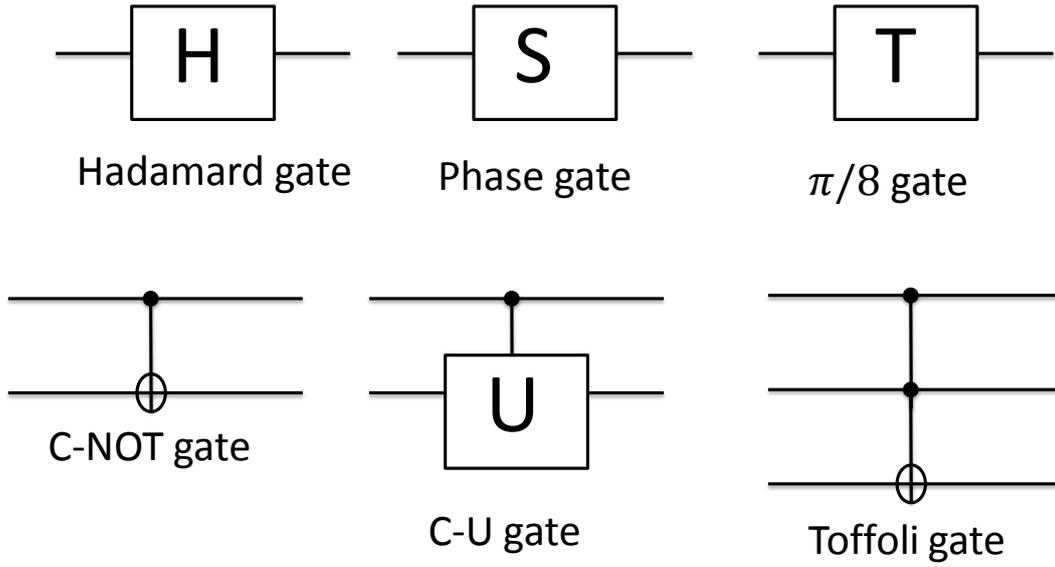
Fig. 1.1: Circuit symbols of various quantum gates

1.1.4 Quantum gates

An arbitrary unitary operator acting on d-dimensional Hilbert space, can be approximated to arbitrary precision in terms of a set of universal gates i.e., C-NOT gate, Hadamard gate, $\pi/8$ gate, and phase gate [NC10]. C-NOT gate, Hadamard gate, Toffoli gate, and phase gate is also a universal set but the proof showing that this set is universal is not as appealing as that of the previous set [NC10].

Hadamard gate: $H = (\sigma_z + \sigma_x)/\sqrt{2}$. Phase gate: $S = |0\rangle\langle0| + i|1\rangle\langle1|$. $\pi/8$ gate: $T = |0\rangle\langle0| + e^{i\pi/4}|1\rangle\langle1|$. C-NOT (controlled NOT) gate: $|0\rangle\langle0| \otimes \mathbb{1}_2 + |1\rangle\langle1| \otimes \sigma_x$. Toffoli gate: $(\mathbb{1}_4 - |11\rangle\langle11|) \otimes \mathbb{1}_2 + |11\rangle\langle11| \otimes \sigma_x$. C-U (controlled U) gate: $|0\rangle\langle0| \otimes \mathbb{1}_2 + |1\rangle\langle1| \otimes U$. [NC10]. The circuit symbols of these gates has been shown in Fig. 1.1.

1.2 Basics of nuclear magnetic resonance (NMR)

Consider the ^{1}H nuclei present in water, benzene etc. It is a spin-1/2 particle (proton). It has three quarks, and quark is a spin-1/2 particle. Then the total spin quantum number of proton, using addition of angular momentum algebra, turns out to be 1/2 (other combinations are rare) [Lev08].

1.2.1 Spin temperature and thermodynamic/ordinary/bath/kinetic temperature

Absolute temperature T is a dimensionless parameter defined as

$$1/T = \frac{\partial S}{\partial E} \tag{1.6}$$

where entropy $S = k_{\mathrm{B}} \ln \Omega(E)$, $\Omega(E)$ is the number of states whose energy lies between E and $E + \delta E$, k_{B} is the Boltzmann constant [Rei85]. For all ordinary systems where one takes into account the kinetic energy of the particles, there is no upper bound on the possible energy of the system (a lower bound, of course, exists, namely the quantum mechanical ground state energy). In such ordinary cases $\Omega(E) \propto E^f$ where f is the number of degrees of freedom of the system, and hence $\Omega(E)$ increases monotonically with E. Hence from the definition (1.6) we get $T > 0$ [Rei85]. Let us call this thermodynamic/ordinary/bath/kinetic temperature. Note that here we are considering f of the order of Avogadro number and the relation $\Omega(E) \propto E^f$ is only an order of magnitude estimate and hence not precise [Rei85].

However if we are not interested in the translational degrees of freedom (i.e., position and momentum), but interested only in spin degrees of freedom (like in NMR), then the system has an upper bound to its possible energy (e.g., all spins polarized anti-parallel

to the static magnetic field) and also a lower bound to its possible energy (e.g., all spins polarized parallel to the static magnetic field). Correspondingly the total number of states (irrespective of energy) available to the system is finite. In this case $\Omega_{\mathrm{spin}}(E)$ increases as E increases, reaches a maximum, and then starts decreasing with further increase in energy. Hence from the definition (1.6) we see that, spin temperature T_{spin} can be both positive as well as negative [Rei85, AP58].

The third law of thermodynamics i.e., "The entropy S of a system has the limiting property that as $T \to 0_+$, $S \to S_0$ where S_0 is a constant independent of all parameters of the particular system." [Rei85], applies to both spin temperature as well as ordinary temperature. Note that S_0 is independent of all parameters of the particular system in the widest sense i.e., independent of spatial arrangement of its atoms or of the interaction between them [Rei85].

1.2.2 Zeeman splitting

In the absence of external magnetic field, Hamiltonian of ^{1}H is $0 \times \mathbb{1}_2$ (null matrix) whose eigenvalue zero is two fold degenerate. Any state (Eq. (1.1)) is an eigenstate of $0 \times \mathbb{1}_2$ and hence no time evolution. Degeneracy is a consequence of symmetry [OP09]. When we switch on the uniform external magnetic field (z-axis or quantization axis is taken to be along this field), symmetry is broken by introducing a preferred spatial direction which in turn fixes the basis in the degenerate subspace. Consequently the Hamiltonian is given by

$$H = -\vec{\mu}.\vec{B}_{\mathrm{loc}} \approx \omega^0 I_z \tag{1.7}$$

where $\vec{B}_{\mathrm{loc}} \approx B^0(1+\delta)\hat{z}$ (using secular approximation in isotropic liquids) is the local magnetic field at the site of the nuclei, B^0 is the external magnetic field, δ is the chemical
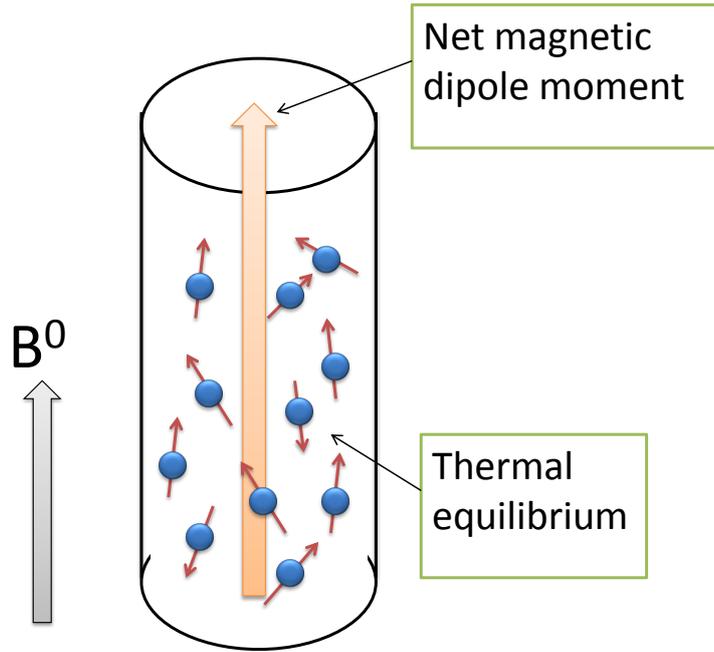
Fig. 1.2: Thermal equilibrium state of the nuclear spins in the presence of Zeeman field.

shift, $\vec{\mu} = \gamma(I_x\hat{x} + I_y\hat{y} + I_z\hat{z})$ is the magnetic dipole moment vector operator, $I_x = \sigma_x/2$ is the x-component of the spin angular momentum vector operator, γ is the gyromagnetic ratio, and $\omega^0 = -\gamma B^0(1 + \delta)$ is the chemically shifted Larmor precession frequency of the nuclei in radians per second [Lev08]. Consequently the degeneracy is broken, and from Eq. (1.7) we see that the energy levels are split by $\omega_0/2 - (-\omega_0/2) = \omega_0$ (in units of $\hbar$, the 'natural unit'; scalars and operators corresponding to angular momentum and energy, in 'natural units' has to be multiplied by $\hbar$ to obtain the corresponding quantities in SI units [Lev08]).

1.2.3 Thermal equilibrium state

In a typical NMR sample of one qubit registers, there will be approximately 10^{15} noninteracting, randomly polarized spin-1/2 particles (see Fig. 1.2). As NMR qubits at room temperature are distinguishable (via spatial location of well separated wave packets),

we can use Boltzmann distribution to know their statistical properties. Hence their thermal equilibrium state in Zeeman basis, is described by the density matrix

$$\rho_{\text{eq}} = \frac{e^{-H/(k_B T)}}{\text{Tr}(e^{-H/(k_B T)})} \approx \frac{\mathbb{1}_2}{2} + \epsilon I_z = \frac{1+\epsilon}{2}|0\rangle\langle 0| + \frac{1-\epsilon}{2}|1\rangle\langle 1| = (1-\epsilon)\frac{\mathbb{1}_2}{2} + \epsilon|0\rangle\langle 0|$$
$$= \sum_i p_i|\theta_i, \phi_i\rangle\langle\theta_i, \phi_i| \quad (1.8)$$

where the approximation corresponds to high temperature, and secular approximation, $\epsilon(= -\hbar\omega_0/(2k_B T)) \sim 10^{-5}$ is the purity factor [Cav96, Lev08], and $\sum_i p_i = 1$. Note that ground state $|0\rangle$ is slightly more populated than the excited state $|1\rangle$. Hence we get net magnetization even in thermal equilibrium state. Even though spins are randomly oriented, there is no coherence (off diagonal terms). This is explained by the second line in the above equation i.e., no unique decomposition of a mixed density matrix (Eq. (1.5)).

Let $H = \omega_0 I_z$, whose eigenvectors are $|0\rangle, |1\rangle$. Then ρ_{eq} is diagonal in $\{|0\rangle, |1\rangle\}$ basis. Hence according to density matrix description, we should not get any signal without using radio frequency (rf) pulse to tilt the net magnetization (which is lying along z-axis) away from the z-axis. However, we do obtain a weak signal (spin noise) due to incomplete statistical cancellation (which persists even in the limit of number of qubits going to infinity [SKBSS20]), as predicted by Bloch [Blo46, FHLD15, SHHC87]. Does it demonstrate the incompleteness of density matrix description?

1.2.4   Resonance condition

Using rf pulse, we rotate/tilt the net magnetization, initially lying along z-axis (Fig. 1.2), onto x-y plane (Fig. 1.3). Then due to Larmor precession, an emf is induced in the coils, which in turn is amplified and detected as NMR signal. It is interesting to note that, even though the amplitude of oscillating magnetic field in the rf pulse is much
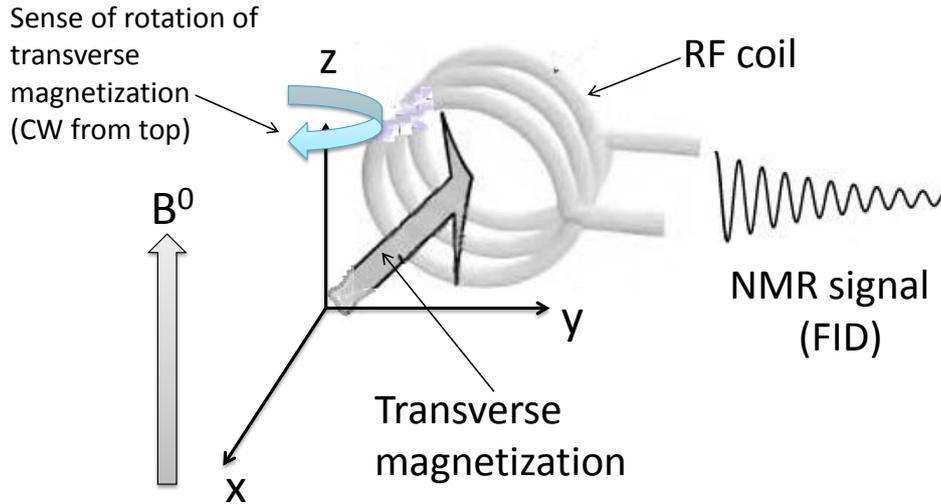
Fig. 1.3: Emf induced by precessing net magnetization, and NMR signal.

smaller than the Zeeman field (B^0), still we can move the net magnetization from z-axis onto the x-y plane. This is made possible by the resonance condition. Hamiltonian corresponding to the rf field acts as perturbation to the Zeeman Hamiltonian, and it connects the two Zeeman states $|0\rangle$ and $|1\rangle$. When the frequency of the rf is equal to the Larmor precession frequency of the nucleus, resonance is achieved and the transition probability (from $|0\rangle$ to $|1\rangle$) becomes one after certain time (see Fig. 1.4) [CTDL05]. This effect is same as that in a child's swing, wherein if the driving frequency is same as the natural frequency of oscillation of the swing, then due to resonance, amplitude of oscillation gets larger and larger with time [Lev08].

1.2.5 Nuclear spin interactions

The nuclear spin Hamiltonian H_{spin} contains only terms that depend on polarization direction of nuclear spin. The electronic motions are very rapid and hence nuclear spins sense only the average electric and magnetic fields produced by electrons. This approximation is known as spin Hamiltonian hypothesis [Lev08]. Consequently we have

13
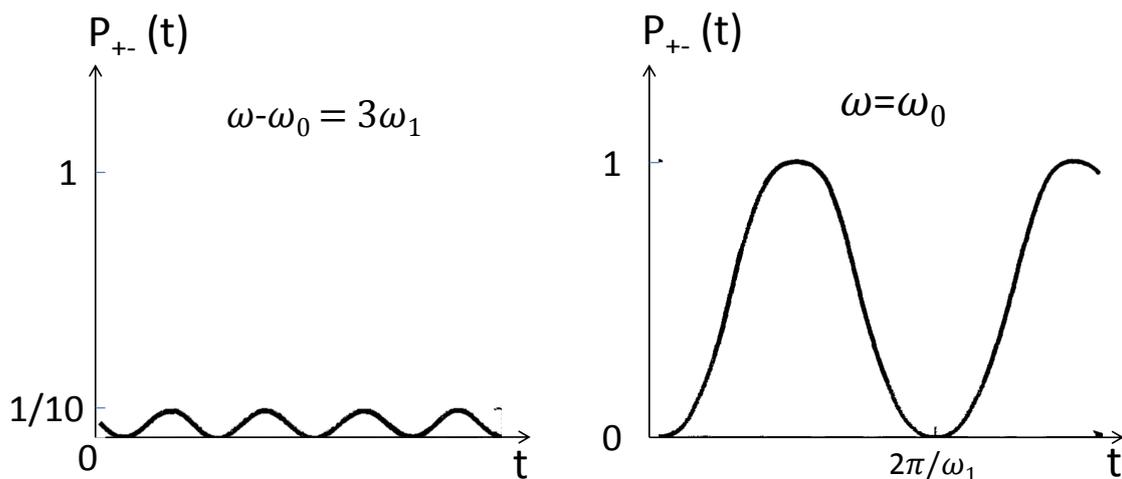
Fig. 1.4: Transition probability (y-axis) corresponding to off-resonance (left figure) and on-resonance (right figure) conditions. x-axis is time.

$H_{\text{spin}} = H_{\text{elec}} + H_{\text{mag}}$ where H_{elec} is due to the electric charge carried by the nucleus placed in the electric field produced by the surrounding electrons, and H_{mag} is due to the interaction of magnetic dipole moment of the nuclear spin (which is proportional to spin angular momentum) with the net magnetic field (at the site of a given nucleus) produced by surrounding electrons, other nuclear spins, and externally applied magnetic field. $H_{\text{elec}} = 0$ for nuclear spin quantum number $= 1/2$. Only for nuclear spin quantum number ≥ 1, $H_{\text{elec}} = H_{\text{elec}}^{\text{quadrupole}}$ [Lev08].

$H_{\text{mag}} = H_{\text{mag}}^{\text{ext}} + H_{\text{mag}}^{\text{int}}$. $H_{\text{mag}}^{\text{ext}} = H_{\text{static}} + H_{\text{grad}} + H_{\text{rf}}$ where H_{static} is due to the externally applied strong Zeeman uniform magnetic field B^0, H_{grad} is due to the externally applied gradient (non uniform) magnetic field (i.e., pulse field gradient), and H_{rf} is due to the oscillating magnetic field of the radio frequency pulse.

$H_{\text{mag}}^{\text{int}} = H_{\text{CS}} + H_{\text{rot}} + H_{\text{J}} + H_{\text{DD}}$ where H_{CS} is due to the magnetic field produced by the revolving electrons at the site of the nucleus, H_{rot} is due the magnetic field generated at the site of the nucleus due to the rotation of the molecule, H_{J} is due to the interaction

between two nuclear spins assisted by the surrounding electrons, and H_{DD} is due to the direct magnetic dipole-dipole interaction between two nuclear spins. Depending on the experimental context, further details on the Hamiltonian terms are provided in later chapters wherever necessary.

1.2.6 Quantum control

Suppose we want to simulate quantum mechanically the evolution of a quantum state $|\psi_{act}\rangle$ under the unitary operator U_{act}. Then we can encode $|\psi_{act}\rangle$ onto NMR spin state $|\psi_{encode}\rangle$ and decompose $U_{act} = \prod_j U_{act}^j$. Note that there is no unique decomposition of U_{act}. Then U_{act}^j can be realized using the spin Hamiltonian as follows $U_{act}^j \approx U_{encode}^j = \exp(-iH_{\mathrm{spin}}(a_j, b_j, ...)\Delta t_j)$ where $a_j, b_j, ...$ are control parameters [BAM16]. Then the gate fidelity is defined as $F_{gate} := |\mathrm{Tr}(U_{act}^\dagger \prod_j U_{encode}^j)/d|^2$ where d is the dimension of the Hilbert space [BAM16]. Let $\rho'_{act} = |\psi'_{act}\rangle\langle\psi'_{act}|$, and $\rho'_{encode} = |\psi'_{encode}\rangle\langle\psi'_{encode}|$ where $|\psi'_{act}\rangle = U_{act}|\psi_{act}\rangle$, and $|\psi'_{encode}\rangle = \prod_j U_{encode}^j|\psi_{encode}\rangle$. Then the state fidelity is defined as $F_{state} := |\mathrm{Tr}(\rho'_{act}\rho'_{encode})|/\sqrt{\mathrm{Tr}(\rho'^2_{act})\mathrm{Tr}(\rho'^2_{encode})}$ [BAM16]. One can easily generalize the above concepts for mixed states as well.

Various numerical algorithms have been developed to implement the above quantum simulation procedure in an optimal way. They include: Strongly modulating pulses [FPB+02, BBA08, MMK08], GRAPE [Kt05], Krotov [EMT11, RTB+16], and Bang-Bang [BAM16] quantum control algorithms.

1.2.7 Quantum state tomography

Consider an unknown nuclear spin state ρ. To know ρ one has to extract expectation value of certain set of noncommuting observables from the state ρ. Those expectation values will be a function of unknown parameters in ρ. By solving a set of simultaneous

linear constraint equations, we can know the unknown parameters in ρ. This procedure of knowing ρ is known as quantum state tomography [NC10, SRM13]. The state fidelity or correlation of experimentally determined state $\rho_{\exp}$ with the desired target state $\rho_{\tar}$ is defined as $F_{state} := |\text{Tr}(\rho_{\exp}\rho_{\tar})|/\sqrt{\text{Tr}(\rho_{\exp}^2)\text{Tr}(\rho_{\tar}^2)}$.

1.2.8 PPS and POPS

Pseudo pure state (PPS)

In thermal equilibrium, ensemble of nuclear spins are unequally distributed (according to Boltzmann distribution) across various energy levels. Through unitary and nonunitary operations, population of nuclear spins can be redistributed in such a fashion that all energy levels (except ground state) are equally populated and ground state is slightly (one in 10^5) more populated than rest of the energy levels. That is

$$\rho_{\text{eq}} \to \rho_{\text{PPS}} = (1 - \epsilon')\mathbb{1}_{2^N}/2^N + \epsilon'|0\rangle\langle 0|^{\otimes N} \tag{1.9}$$

where N is the number of qubits, $\epsilon' < \epsilon = -\hbar\omega_0/(2^N k_B T) \sim 10^{-5}$. Hence ρ_{PPS} is isomorphic to the pure state $|0\rangle\langle 0|^{\otimes N}$ (because $\mathbb{1}_{2^N}/2^N$ will not contribute to NMR signal) [CFH97, SHC00, PZF+01].

Pair of pseudo pure states (POPS)

When N is large, preparing ρ_{PPS} is difficult as it requires elaborate pulse sequence. Instead, one can easily prepare POPS corresponding to arbitrary N as follows: 1. Depending on which pair of PPS is to be prepared, selective π-pulse is applied on the corresponding peak of the NMR spectrum of the spin system under study. 2. A nonselective read out pulse is applied and free induction decay (FID) acquired. 3. Another

16

experiment is performed with only step-2. 4. The FID's of the two experiments are subtracted and then Fourier transformed to obtain the spectrum corresponding to the desired POPS.

The peak selected in step-1 is a consequence of transition of spins between two energy levels, say, $|1\rangle$ and $|2\rangle$. Then the POPS we obtain will be the following $|1\rangle\langle1| - |2\rangle\langle2|$ [Fun01]. Further, as electronic noise is common to both the preceding two FID's, noise goes away when we subtract the two FID's.

CHAPTER 2

NMR investigation of contextuality in a quantum harmonic oscillator via pseudospin mapping

"Is the moon there when nobody looks ?"- Albert Einstein [Mer85]

2.1 Abstract

Physical potentials are routinely approximated to harmonic potentials. Hence it is important to know when a quantum harmonic oscillator (QHO) behaves quantum mechanically and when classically. Recently Su *et al.* [Phys. Rev. A **85**, 052126 (2012)] have theoretically shown that QHO exhibits quantum contextuality (QC) for a certain set of pseudospin observables. Here we encode the four energy eigenstates of a QHO onto four Zeeman product states of a pair of spin-1/2 nuclei. Using the techniques of NMR quantum information processing, we then demonstrate the violation of both state-dependent and state-independent inequalities arising from the noncontextual hidden variable model [KKM16].

2.2 Introduction

Quantum contextuality (QC) states that the outcome of the measurement depends not only on the system and the observable but also on the context of the measurement, i.e., on other compatible observables which are measured along with [KS67, Per90, Per91, Per95].

Let us consider a pair of space-like separated entangled particles, with local observables A and C belonging to the first particle, and B and D to the second. We assume that these observables are dichotomic (i.e., can take values ± 1) and that the pairs (A, B), (B, C), (C, D), and (D, A) commute.

Classically, one assigns objective properties to the particles such that D behaves identically on the state of the system irrespective of whether it is measured in the context of A or in the context of C [EPR35, Mer90]. (Note that corresponding quantum mechanical A and C are not compatible.) Such measurements are said to be *context independent*. Classically, one can pre-assign values (a, c) to (A, C) of the first particle independent of the measurement carried out on the second particle. Similarly, for the second particle one can pre-assign values (b, d) to (B, D) independent of the measurement carried out on the first particle. In these pre-assignments, implicit is the assumption of noncontextual hidden variables, which predict definite measurement outcomes independent of the measuring arrangement. If we pre-assign values to observables such that $A, B, C, D = \pm 1$, it follows that $AB + CB + CD - AD = \pm 2$ and the expectation value,

$$
\begin{aligned}
\mathbf{I} \quad &= \langle AB + CB + CD - AD \rangle \\
&= \langle AB \rangle + \langle CB \rangle + \langle CD \rangle - \langle AD \rangle \leq 2
\end{aligned} \tag{2.1}
$$

[NC10]. This inequality often known as CHSH inequality arises from noncontextual

hidden variable (NCHV) model and must be satisfied by all classical particles.

Now let us see the implication of the quantum theory. Let Alice and Bob share a large number of singlet states: $(|01\rangle - |10\rangle)/\sqrt{2} = -(|+-\rangle - |-+\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ are eigenstates of Pauli-z operator (σ_z) and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice measures on her qubit either σ_x^A or σ_z^A, while Bob always measures σ_x^B. Let us compare the results of only those measurements in which Alice has obtained the outcome $+1$. If Alice measures σ_z^A, then Bob's qubit collapse to $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$. In this context (i.e., σ_z^A), Bob will get both outcomes ± 1 with equal probability. On the other hand, if Alice measures σ_x^A on her qubit, then Bob's qubit collapses to $|-\rangle$ and in this context (i.e., σ_x^A), Bob will always get the outcome -1 (σ_x^A and σ_x^B are perfectly anticorrelated). Hence the context dependency. This shows that, quantum nonlocality is only a special case of quantum contextuality [GHH$^+$14, Cav18]. That is when we have two entangled particles which are space-like separated, quantum contextuality manifests itself as quantum nonlocality. This can be further justified by the fact that quantum contextuality can be observed even in a single three level quantum system (qutrit) [KS67, KSS$^+$12, DDA16]. Violation of NCHV inequality in the case of a qutrit, violates classical notion of noncontextuality (which says, outcomes of the observables are pre-assigned even before performing the measurement, and measurement just reveals them, and hence outcomes are independent of the measurement context), but it may not violate the classical notion of realism (which says "each individual outcome of a measurement is causally determined by supplementary variables (the so-called hidden variables) that together with ψ completely specify the state of an individual quantum entity (deterministic realist ingredient)." [Hom97]; realism also means that there exists an objective external world independent of the observer.). When we have two entangled particles which are space-like separated, QC manifests itself as quantum nonlocality, and we observe violation of Bell's inequality. Locality is a consequence of noncontextuality, but the converse is not true, e.g., Bohmian

mechanics which is a contextual hidden variable model (in which value obtained by a measurement is a function of the pre-measurement value as well as the measurement context (i.e., nonlocal hidden variable)) can satisfy the locality condition (at the statistical level but not at the level of individual measurement outcomes) [Hom97]. Hence violation of classical notion of noncontextuality implies/manifests as violation of Einstein locality/separability in the context of entangled particles (i.e., Bell inequality violation), and rules out local hidden variable description of quantum mechanics (but it does not rule out nonlocal hidden variable description of quantum mechanics e.g., Bohmian mechanics is a nonlocal realistic (hidden variable) description of quantum mechanics).

Applications of quantum contextuality: Quantum contextuality based quantum cryptographic protocols [SBA17]; quantum nonlocality (a special case of quantum contextuality) has wide applications in quantum communication like teleportation [NC10], cryptography [Eke91]; measurement based quantum computation [FRB18] etc.

Here we experimentally investigate QC of a quantum harmonic oscillator (QHO). There are a variety of quantum systems whose potentials are approximated by QHO. Consider for example the quantized electromagnetic field used to manipulate a qubit in cavity quantum electrodynamics [WVEB06]. Recently, QC in QHO has been theoretically studied by Su *et al.* [SCW⁺12] by mapping four lowermost QHO energy eigenstates onto four pseudospin states. Such states can be encoded onto qubit states, and QC can be studied by realizing the measurements of appropriate observables. In this work, we realize this study using a nuclear magnetic resonance (NMR) quantum simulator [CFH97].

In the following section 2.3 we shall revisit the formulation of Su et. al., and in section 2.4, we describe the experimental demonstration of state-dependent and state-independent QC using an NMR system. Finally we conclude in section 2.5.

2.3 Theory

Su *et.al.* [SCW+12] have theoretically studied QC of energy eigenstates of 1D-QHO by introducing two sets of pseudo-spin operators,

$$\mathbf{\Gamma} = (\Gamma_x, \Gamma_y, \Gamma_z), \quad \mathbf{\Gamma}' = (\Gamma'_x, \Gamma'_y, \Gamma'_z)$$

with components,

$$\Gamma_x = \sigma_x \otimes \mathbb{1}_2, \Gamma_y = \sigma_z \otimes \sigma_y, \Gamma_z = -\sigma_y \otimes \sigma_y,$$
$$\Gamma'_x = \sigma_x \otimes \sigma_z, \Gamma'_y = \mathbb{1}_2 \otimes \sigma_y, \Gamma'_z = -\sigma_x \otimes \sigma_x, \tag{2.2}$$

where $\mathbb{1}_2$ is 2×2 identity matrix. Energy eigenstates of QHO satisfy the following relations [CTDL05]

$$H|n\rangle = (n + 1/2)\hbar\omega|n\rangle, a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle, a|n\rangle = \sqrt{n}|n-1\rangle, a|0\rangle = 0, \tag{2.3}$$

where H is the Hamiltonian, a and $a^\dagger$ are annihilation and creation operators respectively, and $n = 0, 1, 2, ...$ Further we can rewrite [SCW+12]

$$\Gamma_x = |0\rangle\langle 2| + |1\rangle\langle 3| + |2\rangle\langle 0| + |3\rangle\langle 1|. \tag{2.4}$$

Substituting Eqs. (2.3) into Eq. (2.4) one can express Γ_x in terms $a, a^\dagger$ i.e.,

$$\Gamma_x = |0\rangle\langle 0|a^2/\sqrt{2} + a^\dagger|0\rangle\langle 0|a^3/\sqrt{6} + a^{\dagger 2}|0\rangle\langle 0|/\sqrt{2} + a^{\dagger 3}|0\rangle\langle 0|a/\sqrt{6}. \tag{2.5}$$

Similarly one can express other observables in Eqs. (2.2) in terms of $a, a^\dagger$.

Using these operators they defined the following observables which are unitary, Hermi-

22

tian and nonlocal (in general):

$$A = \Gamma_x = \sigma_x \otimes \mathbb{1}_2,$$

$$B = \Gamma'_x \cos\beta + \Gamma'_z \sin\beta = \sigma_x \otimes (\sigma_z \cos\beta - \sigma_x \sin\beta),$$

$$C = \Gamma_z = -\sigma_y \otimes \sigma_y,$$

$$D = \Gamma'_x \cos\eta + \Gamma'_z \sin\eta = \sigma_x \otimes (\sigma_z \cos\eta - \sigma_x \sin\eta). \tag{2.6}$$

Note that before mapping QHO energy eigenstates onto NMR two qubit states, it does not make sense to call the operators in Eq. (2.6) nonlocal. However it does make sense after the mapping. This is because the two spin-1/2 nuclei are separated in space, and hence the notion of nonlocal/global operations acting on the global space of two qubit system, makes sense. As the spatial separation between nuclei is very small, one can realize nonlocal gates, measurements etc. in NMR. The products which form the inequality expression (2.1) are

$$AB = \mathbb{1}_2 \otimes (\cos\beta \ \sigma_z - \sin\beta \ \sigma_x),$$

$$BC = -\sigma_z \otimes (\cos\beta \ \sigma_x + \sin\beta \ \sigma_z),$$

$$CD = -\sigma_z \otimes (\cos\eta \ \sigma_x + \sin\eta \ \sigma_z),$$

$$DA = \mathbb{1}_2 \otimes (\cos\eta \ \sigma_z - \sin\eta \ \sigma_x). \tag{2.7}$$

Here the following commutation relations hold: $[\Gamma_i, \Gamma'_j] = 0$ $(i, j = x, y, z)$, $[\Gamma_x, \Gamma_y] = 2i\Gamma_z$, $[\Gamma'_x, \Gamma'_y] = 2i\Gamma'_z$, and similar relations with cyclic permutations of x, y, z. The observables A, B, C, D have degenerate eigenvalues ± 1, with (A, B), (B, C), (C, D),

and (D, A) forming compatible pairs. Su *et.al.* [SCW$^+$12] have shown that,

$$\mathbf{I}^{QM}_{|l\rangle_{QHO}} = 2\sqrt{2} > 2, \text{ when, } (\beta, \eta)_l = \begin{cases} (-\pi/4, -3\pi/4)_0 \\ (3\pi/4, \pi/4)_1 \\ (\pi/4, 3\pi/4)_2 \\ (-3\pi/4, -\pi/4)_3 \end{cases} \tag{2.8}$$

where, $\mathbf{I}^{QM}_{|l\rangle_{QHO}}$ is the expression on LHS of inequality (2.1) for $l = 0, 1, 2$ and 3, and, $|0\rangle_{QHO}, |1\rangle_{QHO}, |2\rangle_{QHO}$ and $|3\rangle_{QHO}$ are the first four energy eigenstates of 1D-QHO. Thus QHO violates the inequality (2.1) for certain observables and thereby exhibits QC.

It is well known that only certain two-particle states violate the CHSH inequality (2.1). As shown in [Hom97, CFS73] factorable states always satisfy inequality (2.1) for local observables, which are of the form $P \otimes \mathbb{1}_2$ or $\mathbb{1}_2 \otimes Q$ [Aud07]. With maximally mixed state $(\mathbb{1}_2/2 \otimes \mathbb{1}_2/2)$ the inequality (2.1) is satisfied even with nonlocal observables in eq. (2.6), which are of the form $P \otimes Q$ measured nonlocally/jointly [Aud07], which is obvious from the fact that all the products in eq. (2.7) are traceless. However, if the initial state is nonfactorable, we can always find observables such that inequality (2.1) is violated [Hom97]. Although the pseudospin states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, are factorable, they still violate ineq. (2.1) since the observables in eq. (2.6) are nonlocal. Thus, we observe that even when a system is in an unentangled/separable state, measurements of nonlocal observables may lead to violation of noncontextuality inequality [GKC$^+$10].

State independent QC: There exist stronger inequalities obtained from NCHV models which is violated by all states, including separable or maximally mixed states. If the initial state is maximally mixed, entanglement cannot be created by measuring whatever observable (local or nonlocal). This shows that entanglement is not necessary in general

even in a bipartite system, to exhibit QC. In this sense, it can be argued that, QC is more fundamental or general than entanglement. Any system whose Hilbert space has dimension > 2 exhibits QC [KS67]. Even a *single* spin-1 particle (where entanglement has no meaning as far as spin degree of freedom is concerned) also exhibits QC [KSS$^+$12, DDA16].

2.4 Experiment

2.4.1 State dependent contextuality

To experimentally study the inequality (2.1), we need to realize the following processes:

(i) To physically map various energy eigenstates of 1D-QHO: We encode the first four energy eigenstates $\{|0\rangle_{QHO}, |1\rangle_{QHO}, |2\rangle_{QHO}, |3\rangle_{QHO}\}$ onto the four Zeeman energy eigenstates $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ of a pair of spin-1/2 nuclei (i.e., two qubits) precessing in external static magnetic field. In fact any four arbitrarily chosen energy eigenstates of 1D-QHO and also their superposition states exhibit QC [SCW$^+$12].

(ii) To extract the joint expectation values for operators AB, BC, CD, and DA: The Moussa circuit shown in Fig. 2.1 [MRCL10, JSK$^+$14], is used to extract the expectation values of observables in a joint measurement. Since this protocol needs an ancillary qubit, in all we need to have three qubits with sufficiently long coherence times.

The three qubits for this experiment were provided by the three ^{19}F nuclear spins of trifluoroiodoethylene (Fig. 2.2(a)) dissolved in acetone-D6. The Hamiltonian parameters of the spin system are given in Fig. 2.2(b). The effective ^{19}F spin-spin (T_2^*) and
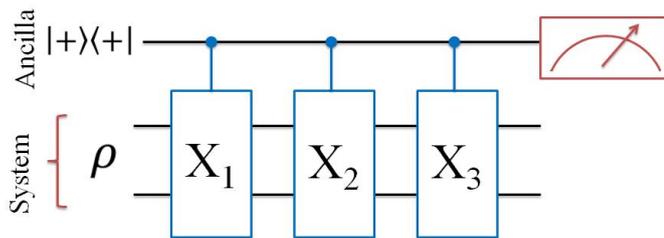
Fig. 2.1: Moussa Protocol for extracting expectation value of the joint observable $X_1 X_2 X_3$ i.e. $\langle X_1 X_2 X_3 \rangle$. Here X_i's are mutually commuting unitary observables. $\langle \sigma_x \otimes \mathbb{1}_2 \otimes \mathbb{1}_2 \rangle_{\rho_{\text{final}}^{\text{as}}} = \langle X_1 X_2 X_3 \rangle_\rho$ where $\rho_{\text{final}}^{\text{as}}$ is the ancilla-system final state after applying all the unitary gates [MRCL10]. Note that $\langle \sigma_x \otimes \mathbb{1}_2 \otimes \mathbb{1}_2 \rangle_{\rho_{\text{final}}^{\text{as}}} = \langle \sigma_x \rangle_{\rho_{\text{final}}^{\text{a}}}$ where $\rho_{\text{final}}^{\text{a}} = \text{Tr}_{\text{system}}(\rho_{\text{final}}^{\text{as}})$ [CTDL05].

spin-lattice (T_1) relaxation time constants were about 0.8 and 6.3 s respectively. The experiments were carried out at an ambient temperature of 290 K on a 500 MHz Bruker UltraShield NMR spectrometer.

The thermal equilibrium state for the three spin system, under high temperature and high field approximation [Lev08], is

$$\rho_{\text{eq}} = \frac{\mathbb{1}_8}{8} + \epsilon \sum_{i=1}^{3} I_{iz} \tag{2.9}$$

where, $\mathbb{1}_8$ is an 8×8 identity matrix, $I_{iz} = \mathbb{1}_{2^{i-1}} \otimes \sigma_z/2 \otimes \mathbb{1}_{2^{3-i}}$ are spin angular momentum operators, and the purity factor $\epsilon = \hbar \gamma B_0/(8 k_B T)$ is the ratio of the Zeeman energy gap to the thermal energy [Cav96]. Note that under high magnetic field approximation we neglect chemical shifts. Unitary operation has no effect on the identity part, but modifies only the traceless deviation part. By applying a series of unitary and nonunitary operators (pulse sequence shown in Fig. 2.2 [MMK08]), it is possible to transform the equilibrium state to a pseudopure state

$$\rho_{\text{pps}} = (1 - \epsilon') \frac{\mathbb{1}_8}{8} + \epsilon' |000\rangle \langle 000| = \frac{\mathbb{1}_8}{8} + \epsilon' \Delta \rho_{|000\rangle} \tag{2.10}$$

26
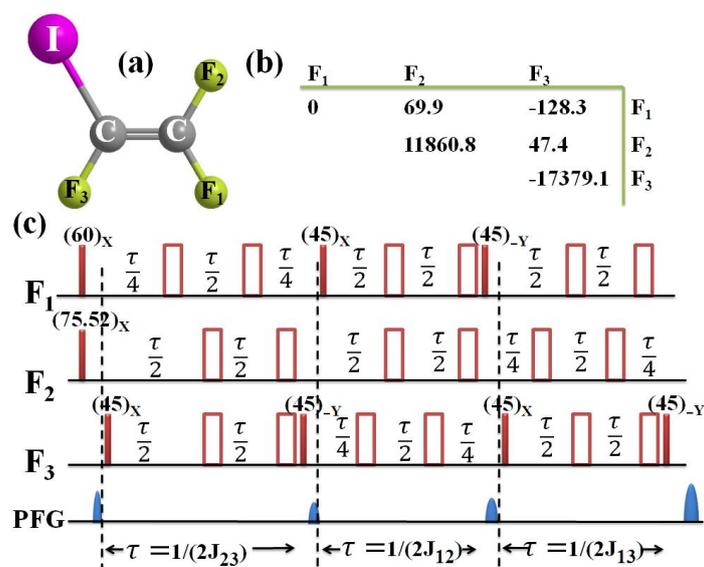
Fig. 2.2: (a) Molecular Structure, (b) resonance off-sets (diagonal elements) and J-couplings (off-diagonal elements) in Hz of trifluoroiodoethylene, and (c) pulse sequence for pseudo-pure state preparation. In (c), 180_x pulses are represented by unshaded rectangles, and other pulses by shaded rectangles with tilt-angles and phases as indicated. Lowest row consists of Pulsed Field Gradients (PFG) used to destroy the transverse magnetization.

which is isomorphic to the pure state $|000\rangle$ [CFH97] up to some purity $\epsilon' < \epsilon$. In the pseudopure state, the traceless deviation part has the form

$$\Delta\rho_{|000\rangle} = \quad \frac{1}{4}(I_{1z} + I_{2z} + I_{3z} + 2I_{1z}I_{2z}$$
$$+2I_{2z}I_{3z} + 2I_{1z}I_{3z} + 4I_{1z}I_{2z}I_{3z}). \tag{2.11}$$

The first spin, F_1, is used as an ancilla qubit, and the other spins, F_2 and F_3, as the system qubits (see fig. 2.1). The initial Hadamard gate on the first spin prepares $\rho_{|+00\rangle}$. To measure $\langle AB \rangle_{|00\rangle}$, we apply the controlled operations corresponding to A and B as indicated in the circuit in Fig. 2.1. The transverse magnetization of the ancilla qubit will be proportional to the expectation value $\langle AB \rangle_{|00\rangle}$ [MRCL10]. The absolute value of $\langle AB \rangle_{|00\rangle}$ is estimated by normalizing the value obtained in the above experiment with that obtained from a reference experiment having no controlled operations. Similarly we can measure other expectation values $\langle BC \rangle_{|00\rangle}$, $\langle CD \rangle_{|00\rangle}$, and $\langle AD \rangle_{|00\rangle}$, and determine the value of $\mathbf{I}_0$. Other values $\mathbf{I}_l$ are obtained by preparing the corresponding pseudopure states $\rho_{|+01\rangle}$, $\rho_{|+10\rangle}$, and $\rho_{|+11\rangle}$ and applying the circuit in Fig. 2.1, in each case.

In our experiments, all the controlled operations were realized by numerically optimized radio frequency (RF) pulses obtained using GRAPE technique [Kt05]. Each pair of controlled operations in the circuit in Fig. 2.1 was realized by a GRAPE sequence with a duration of about 23 ms (having RF segments of duration 5 μs) and an average Hilbert-Schmidt fidelity better than 0.99 over 10% variation in the RF amplitude.

We estimated the values for $\mathbf{I}_l$ (2.1), for all the four eigenstates and independently varied both β and η over the range $[-\pi, \pi]$ with increments of $\pi/4$. The results are shown in Fig. 2.3. The maximum experimental values for $\mathbf{I}_0$, $\mathbf{I}_1$, $\mathbf{I}_2$, and $\mathbf{I}_3$ are 2.40 ± 0.02, 2.45 ± 0.02, 2.39 ± 0.02, and 2.42 ± 0.03 respectively. These values being greater than 2 clearly violate the classical bounds and hence prove QC of QHO. However, values
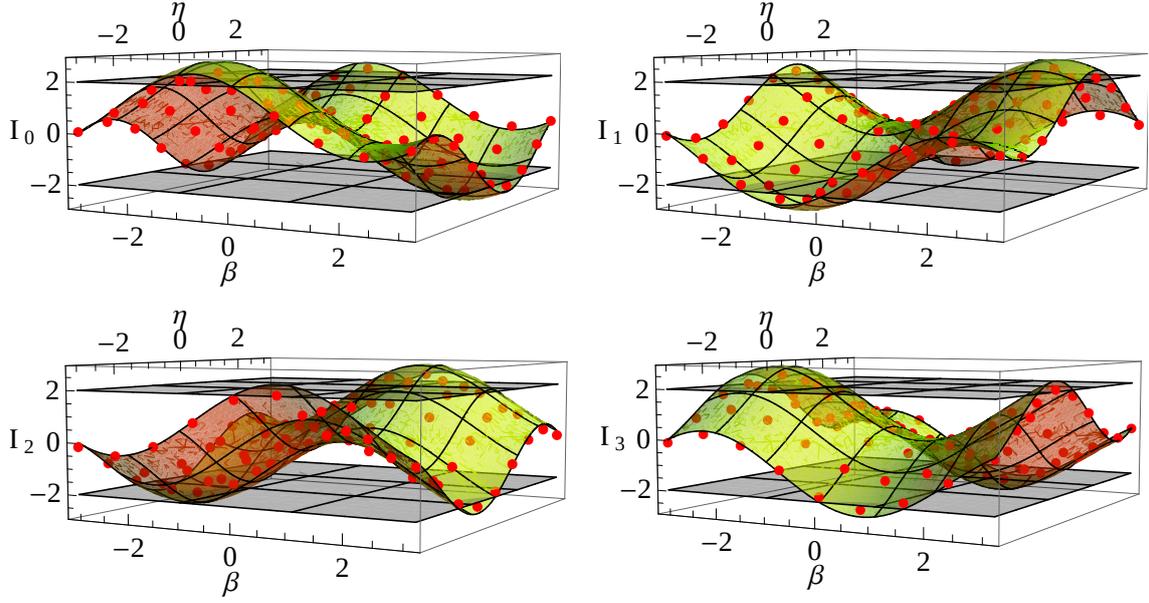
Fig. 2.3: $\mathbf{I}_0$, $\mathbf{I}_1$, $\mathbf{I}_2$, and $\mathbf{I}_3$ represent evaluation of expression (2.1) for eigenstates $|0\rangle_{QHO}, |1\rangle_{QHO}, |2\rangle_{QHO}$, and $|3\rangle_{QHO}$ respectively. The experimental values are shown by red dots and theoretical surfaces are shown for reference. The flat planes at 2 and -2 correspond to classical bounds.

lower than the maximum theoretical violation (i.e., $2\sqrt{2} \approx 2.83$) are presumably due to the decoherence intrinsic to the quantum system and other experimental imperfections.

2.4.2 State independent contextuality

Su *et.al.* have also studied the state independent contextuality [SCW⁺12, Cab08] by considering the inequality (arising from NCHV model)

$$\langle P_{11}P_{12}P_{13}\rangle + \langle P_{21}P_{22}P_{23}\rangle + \langle P_{31}P_{32}P_{33}\rangle$$

$$+\langle P_{11}P_{21}P_{31}\rangle + \langle P_{12}P_{22}P_{32}\rangle - \langle P_{13}P_{23}P_{33}\rangle \leq 4 \tag{2.12}$$

where P_{ij} are the elements of the matrix P,

$$P = \begin{pmatrix} \Gamma_z & \Gamma'_z & \Gamma_z\Gamma'_z \\ \Gamma'_x & \Gamma_x & \Gamma_x\Gamma'_x \\ \Gamma_z\Gamma'_x & \Gamma_x\Gamma'_z & \Gamma_y\Gamma'_y \end{pmatrix}. \tag{2.13}$$

Here, in each row (column) of the matrix P, every observable commutes with every other. P_{ij} are dichotomic observables with measurement outcomes ± 1. We can verify the inequality (2.12) by preassigning the values ± 1 to each of the observables P_{ij}'s.

Now introducing the operators from expressions (2.2), we find that the product of each row of the matrix P is identity (i.e., $P_{j1}P_{j2}P_{j3} = \mathbb{1}_2$). Similarly, the products along each of the first two columns again become identity. However, the product along the last column, i.e., $P_{13}P_{23}P_{33} = -\mathbb{1}_2$. No preassignment of ± 1 to the various elements of P can satisfy the condition that, product along each row and along the first two columns be $+1$ and that along the last column be -1. This shows that quantum theory is not compatible with NCHV model. Further, the expectation values for the first five operators in expression (2.12) are all $+1$ while that of the last term is -1. Therefore, for an arbitrary state, the quantum upper bound for left hand side of expression (2.12) is 6, while the classical upper bound is 4 [SCW⁺12].

To investigate state-independent QC, we need to measure joint expectation values of three observables. We again use the circuit in Fig. 2.1 for this purpose. Taking advantage of the state independent property of the above mentioned inequality (2.12), we choose thermal equilibrium state (2.9) as the initial state. A $(\pi/2)_y$ pulse was applied on the first spin to prepare the ancilla in a superposition state. Then the state (2.9) transforms to: $(1-4\epsilon)\mathbb{1}_8/8 + \epsilon(|+\rangle\langle+|\otimes\mathbb{1}_2\otimes\mathbb{1}_2) + \epsilon(I_{2z} + I_{3z})$. Note that here the terms $(1-4\epsilon)\mathbb{1}_8/8$ and $\epsilon(I_{2z} + I_{3z})$ will not contribute to the expectation value of the ancilla,

because the ancilla (first qubit) is in a maximally mixed state in these terms (only the $|+\rangle\langle+|$ state of the ancilla contributes), and we measure the ancilla only [MRCL10].

All the controlled P_{ij} operations were realized using the GRAPE sequences having average fidelities better than 0.99 where average was taken over 10% variation in RF amplitude. The total duration of the RF sequences for each term in inequality (2.12) were about 40 ms. Experimentally obtained value of left hand side of inequality (2.12) is 4.81 ± 0.02. Thus we observed a clear violation of the classical bound. However it is still lower than 6, the quantum limit. The reduced violation can again be attributed to decoherence and other experimental imperfections.

2.5 Conclusions

We have experimentally demonstrated the quantum contextuality exhibited by first four energy-eigenstates of a one dimensional quantum harmonic oscillator by mapping them to Zeeman energy-eigenstates of a pair of NMR-qubits. The observables (with continuous parameter (but with discrete spectra)) of the harmonic oscillator are then mapped onto certain pseudospin observables measured on the qubits. We have used Moussa protocol to retrieve the joint expectation values of the observables using an ancillary qubit. Thus our quantum register was based on three mutually interacting spin-1/2 nuclei controlled by NMR techniques. The experimental results clearly violate the classical bound proving contextuality in the quantum harmonic oscillator.

We also studied a state-independent quantum contextuality by measuring a set of expectation values on the thermal equilibrium states of the nuclear spins. Experiments again revealed a clear violation of the classical bound. These results not only establish the validity of quantum theoretical calculations, but also highlight the success of NMR systems as quantum simulators.

CHAPTER 3

Discriminating between Lüders and von Neumann measuring devices: An NMR investigation

"...whereas the ansatz of von Neumann yields a most complicated mixture. The extreme case is provided by 'measurement' of the unit operator. Nothing is revealed about the system, which should survive the 'measurement process' uninfluenced."-G.Lüders [Lö6].

3.1 Abstract

Different proposals exist to describe the quantum state after measuring a *degenerate* observable viz., Lüders and von Neumann state update rules. While the former preserves superpositions in the degenerate subspaces, the latter does not. Even though both rules are valid and realizable, which rule a given measuring device ("Black Box") obeys, depends on its internal details. Recently Hegerfeldt and Mayato [Phys. Rev. A 85, 032116 (2012)] had formulated a protocol to discriminate between the two kinds of measuring devices. Here we have reformulated this protocol for system and measuring qubits. We then experimentally investigated this protocol on an NMR spectrometer, and found that Lüders rule is favored [KSM16].

3.2 Introduction

Quantum measurement paradox lies at the heart of foundations of quantum mechanics [Hom97]. It's an experimental fact that, upon measurement, a quantum state collapses into an eigenstate of the observable being measured. However there is no collapse in the unitary evolution described by Schrödinger equation, and therefore, the collapse has to be imposed from outside the formalism.

Let us assume an observable A_N with discrete and nondegenerate eigenspectrum. In that case, the measurement leads to a collapse of the state to one of the eigenstates of A_N (see Fig. 3.1). On the other hand, if we consider an observable A with a degenerate eigenspectrum, there are two extreme rules to update the state after the measurement. The most commonly used rule was postulated by Gerhart Lüders in 1951 [Lüd51, LÖ6]. According to it, a system existing in a superposition of eigenstates corresponding to the degenerate eigenvalue of A, is unaffected by the measurement such that the superposition in the degenerate subspace is preserved. However, an earlier postulate by von Neumann, proposed in 1932 [vN55], does not preserve such a superposition. In the latter postulate, the measuring device refines the observable A into another commuting observable A' (actual system observable) having a nondegenerate spectrum. The resulting measurement collapses the state to an eigenstate of A', and the original superposition is not preserved under the measurement as if the degeneracy has been lifted [HSM12].

Although, one generally assumes Lüders state update rule implicitly in quantum physics, occasionally one encounters applications of the von Neumann state update rule. One example is in the context of Leggett-Garg inequality in multilevel quantum systems [BE14]. In principle, measurements which are intermediate between Lüders and von Neumann can also be conceived [HSM12, BE14].

Recently, Hegerfeldt and Mayato have proposed a general protocol (HM protocol) to

System	Observable	Measurement	Post-measurement state	Outcome
Quantum State ρ	Nondegenerate A_N	→	<u>Collapse to an eigenstate</u> - No difference between Lüders & von-Neumann	An eigenvalue of A_N
	Degenerate A		<u>Lüders collapse</u>: - Degeneracy respecting - Superposition preserved	An eigenvalue of A
			<u>von-Neumann collapse</u>: - Degeneracy breaking - Superposition not preserved	An eigenvalue of A

Fig. 3.1: Comparison between Lüders and von Neumann measurement postulates.

discriminate between Lüders and von Neumann kind of measuring devices [HSM12]. To explain this protocol we consider an observable A, having two-fold degenerate eigenvalues, say $+1$ and -1 (see Fig. 3.2). The HM protocol involves the following steps: (i) prepare an eigenstate $|\xi_{\text{in}}\rangle$ of A in its degenerate subspace, (ii) let the device measure A, and (iii) characterize the output state. In step (ii) a Lüders measurement will preserve the state, while a von Neumann measurement may not. The last step is simply to determine if the step (ii) has changed the state or not. If the state has changed, we conclude that the device is von Neumann. Else, either the device is of Lüders type, or the chosen initial state $|\xi_{\text{in}}\rangle$ happens to be a nondegenerate eigenstate of the actual system observable A'. To rule out the latter possibility, one may change the initial state and repeat the above steps (Fig. 3.2). This way one can attempt to discriminate between the Lüders and von Neumann measurement devices.

In this work, we reformulate the HM protocol for a quantum register and try to investigate it using experiments. Nuclear spin ensembles in liquid, liquid-crystalline, or solid-state systems have often been chosen as convenient testbeds for studying foundations of quantum physics [SMP88, MRCL10, ARM11, KKM16]. Their main advantages
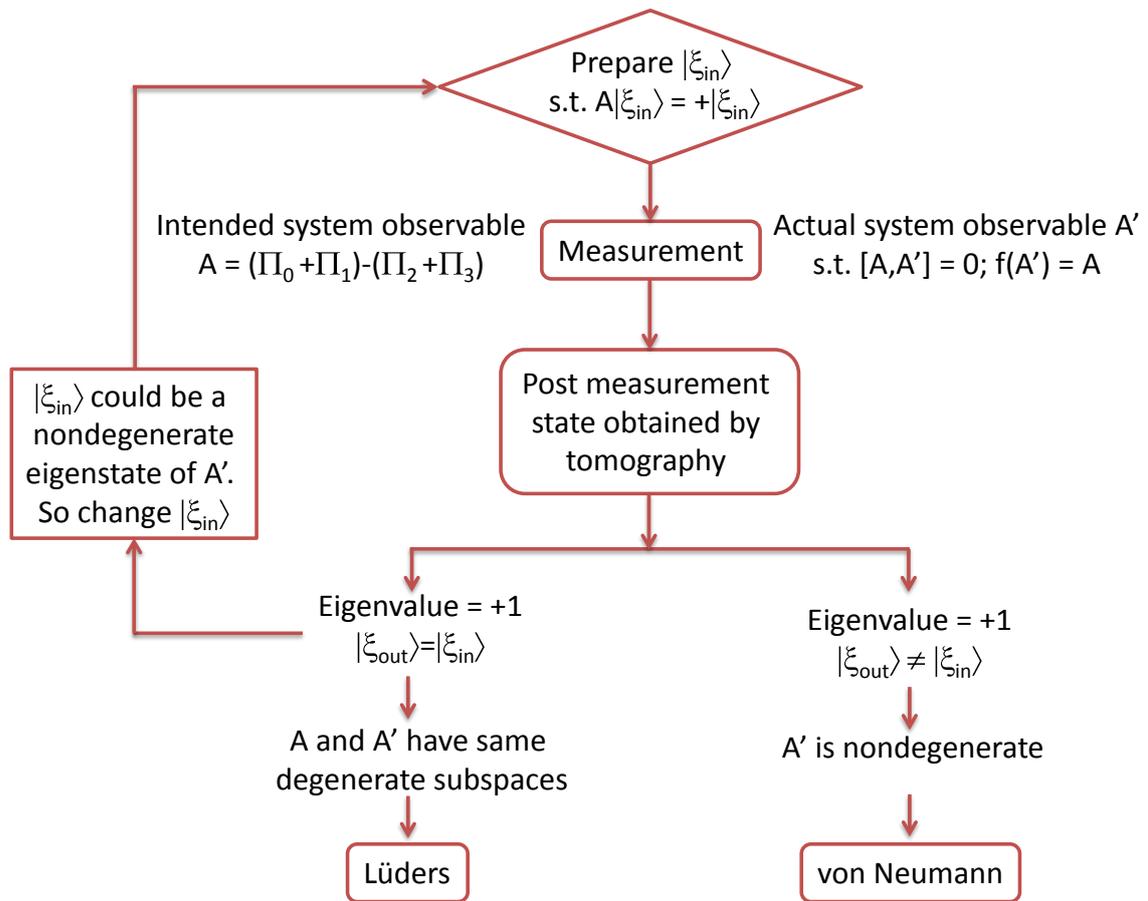
Fig. 3.2: HM protocol for discriminating between Lüders and von Neumann measurements.

are long coherence times and excellent control over quantum dynamics via highly developed nuclear magnetic resonance (NMR) techniques.

In section 3.3, we briefly explain the HM protocol as adapted to an NMR setup. The experimental details to discriminate between the Lüders and von Neumann measuring devices are described in section 3.4. Finally we conclude in section 3.5.

3.3   Theory

For the sake of clarity, and also to match the experimental details described in the next section, we consider a system of two qubits. Since the system is to be measured projectively, dimension of the pointer basis should be greater than or equal to that of the system, and hence we need at least two ancillary qubits. We refer to the ancillary qubits as (1,2) and system qubits as (3,4). We use Zeeman product basis as our computational basis and denote eigenkets of σ_z, the Pauli z-operator, by $|0\rangle$ and $|1\rangle$. We denote the basis vectors of system qubits as

$$|\phi_0\rangle = |00\rangle, |\phi_1\rangle = |01\rangle, |\phi_2\rangle = |10\rangle, |\phi_3\rangle = |11\rangle. \tag{3.1}$$

Let us assume a two-fold degenerate system-observable with spectral decomposition

$$A = (\Pi_0 + \Pi_1) - (\Pi_2 + \Pi_3), \tag{3.2}$$

where the projectors are defined as $\Pi_j = |\chi_j\rangle\langle\chi_j|, |\chi_0\rangle = \alpha_0|\phi_0\rangle + \beta_0|\phi_1\rangle, |\chi_1\rangle = \alpha_1|\phi_0\rangle + \beta_1|\phi_1\rangle, |\chi_2\rangle = \alpha_2|\phi_2\rangle + \beta_2|\phi_3\rangle, |\chi_3\rangle = \alpha_3|\phi_2\rangle + \beta_3|\phi_3\rangle$ are eigenvectors of A. The projectors have the property $\Pi_k\Pi_l = \delta_{kl}\Pi_k$ where δ_{kl} is the Kronecker delta function. We note that A has no unique spectral decomposition due to the degeneracy.

36

We consider a measurement model, wherein a quantum system being measured undergoes a joint evolution with the measuring device, ultimately forming an entangled state. When the measuring device collapses to a particular pointer state, the system also collapses to the corresponding eigenstate. Let Q be the observable corresponding to the ancilla (measuring device) and g be the system-ancilla interaction strength. The joint evolution is then of the form

$$U_{\mathrm{int}} = \exp(-i\mathcal{H}_{\mathrm{int}}\tau), \tag{3.3}$$

where $\mathcal{H}_{\mathrm{int}} = g\, Q \otimes A$ is the interaction Hamiltonian in units of angular frequency.

To fix the basis inside a degenerate subspace, we should choose a nondegenerate observable A' which commutes with A, so that they are simultaneously diagonalizable and hence we can find a common eigenbasis. For simplicity we choose the computational basis $\{|\phi_j\rangle\}$ as the common eigenbasis. Then the observable A' must have the following spectral decomposition

$$A' = \sum_{j=0}^{3} a'_j P_j, \tag{3.4}$$

where $P_j = |\phi_j\rangle\langle\phi_j|$ and the nondegenerate eigenvalues a'_j are yet to be determined.

Let us assume the device to be von Neumann which refines the degenerate observable A that is being measured, into a nondegenerate observable A', via a mapping $f(A') = A$. As the refined observable A' has nondegenerate eigenvalues and commutes with A, it fixes the basis inside the degenerate subspace. However, the choice of A' is not unique, i.e., any orthonormal basis inside the degenerate subspace can be nondegenerate eigenkets of A', and the von Neumann device has the freedom to choose among them [vN55].

The measurement outcome is passed via the refining function f, such that $f(a'_0) = f(a'_1) = +1$ and $f(a'_2) = f(a'_3) = -1$. Hence the outcome is same as if A is being measured. To projectively measure the observable A', the measuring device has to jointly evolve with the system under the interaction Hamiltonian,

$$\mathcal{H}'_{\text{int}} = g\, Q \otimes A'. \tag{3.5}$$

For instance, we choose $Q = q_1 \sigma_{1z} + q_2 \sigma_{2z}$, where $\sigma_{1z} = \sigma_z \otimes \mathbb{1}_2$, $\sigma_{2z} = \mathbb{1}_2 \otimes \sigma_z$ and $\mathbb{1}_2$ is 2×2 identity operator. The joint evolution between the measuring device (ancillary qubits) and the system is described by the unitary operator

$$U'_{\text{int}} = \exp(-i\mathcal{H}'_{\text{int}}\tau), \tag{3.6}$$

where τ is duration of the evolution.

If each of the quantum register is initially prepared in $|\Phi_0\rangle = |{+}{+}{+}{+}\rangle$, with $|+\rangle =$
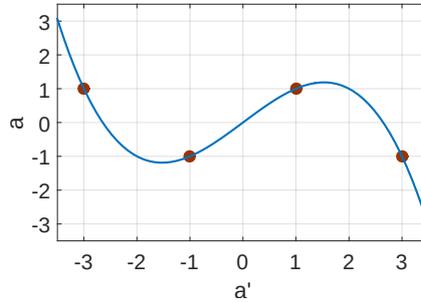
Fig. 3.3: An interpolating function $a = f(a') = (-a'^3 + 7a')/6$ mapping the nondegenerate eigenvalues a' of A' onto degenerate eigenvalues a of A.

$(|0\rangle + |1\rangle)/\sqrt{2}$, the state after the joint evolution is given by

$$
\begin{aligned}
U'_{\text{int}}|\Phi_0\rangle &= \frac{1}{2}\bigg(e^{-iga'_0 Q\tau}|++\rangle|\phi_0\rangle + e^{-iga'_1 Q\tau}|++\rangle|\phi_1\rangle + \\
&\qquad e^{-iga'_2 Q\tau}|++\rangle|\phi_2\rangle + e^{-iga'_3 Q\tau}|++\rangle|\phi_3\rangle\bigg) \\
&= \frac{1}{2}\sum_{j=0}^{3}|\psi_j\rangle|\phi_j\rangle,
\end{aligned}
\tag{3.7}
$$

where $|\phi_j\rangle$ are as defined in Eqs. (3.1) and $|\psi_j\rangle = \exp(-iga'_j Q\tau)|++\rangle$ represent states of the ancillary qubits. To realize the projective measurement, the pointer basis $\{|\psi_j\rangle\}$ must be orthonormal. Imposing the mutual orthogonality condition results in trigonometric constraint equations leading to a set of possible solutions. One such possible solution is

$$
\begin{array}{c|c}
a'_0 = -a'_2 = -3 & q_1 = \pi/(4g\tau) \\
a'_1 = -a'_3 = 1 & q_2 = -q_1/2.
\end{array}
\tag{3.8}
$$

Again, the von Neumann measuring device has the freedom to choose a particular pointer basis among several possible ones. Substituting the above values in Eq. (3.4), we obtain,

$$
A' = -3P_0 + P_1 + 3P_2 - P_3,
\tag{3.9}
$$

which is obviously nondegenerate in the computational basis. The refining function f can now be setup by interpolating the eigenvalue distribution (see Fig. 3.3). For the above example, we find a possible map to be $f(A') = (-A'^3 + 7A')/6 = A$.

The quantum circuit for discriminating Lüders and von Neumann devices, illustrated in Fig. 3.4, involves four qubits each of which is initialized in state $|+\rangle$. If the device is Lüders, the system undergoes a joint evolution U_{int} with the ancilla, resulting in the
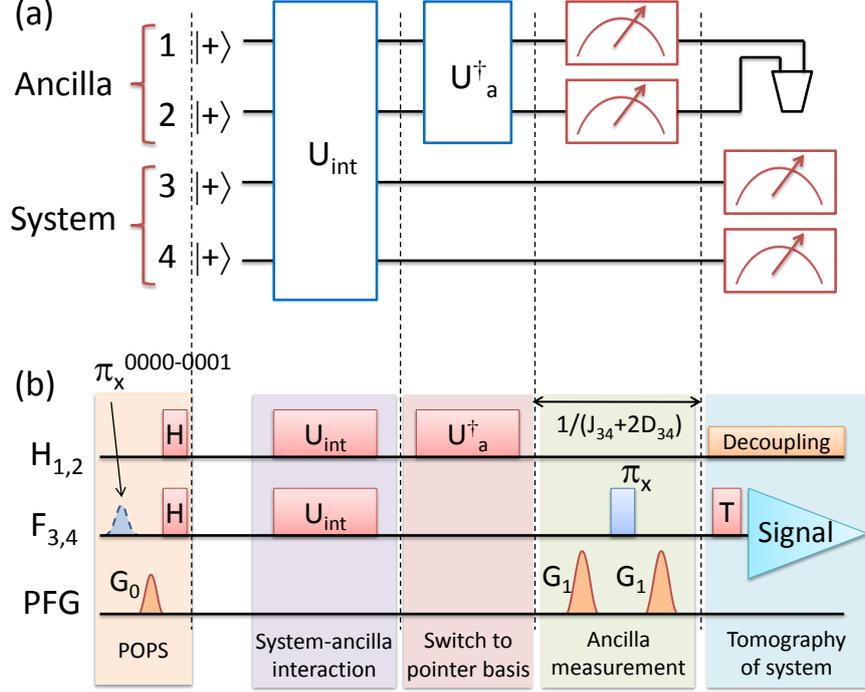
Fig. 3.4: (a) Quantum circuit to discriminate Lüders and von Neumann devices. (b) The NMR pulse-scheme to implement the circuit in (a).

state

$$
\begin{aligned}
U_{\text{int}}|\Phi_0\rangle &= \frac{1}{\sqrt{2}}\left(e^{-igQ\tau}|{++}\rangle\frac{d_0|\chi_0\rangle + d_1|\chi_1\rangle}{\sqrt{2}} + \right. \\
&\qquad \left. e^{igQ\tau}|{++}\rangle\frac{d_2|\chi_2\rangle + d_3|\chi_3\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2}}\left(|\psi_1\rangle\frac{|\phi_0\rangle + |\phi_1\rangle}{\sqrt{2}} + |\psi_3\rangle\frac{|\phi_2\rangle + |\phi_3\rangle}{\sqrt{2}}\right),
\end{aligned}
\tag{3.10}
$$

where the coefficients d_j depend on the choice of $|\chi_j\rangle$ (defined after Eq. (3.2)). Note that the Lüders device may also map A to A' which is of the form $A' = a'_1(\Pi_0 + \Pi_1) + a'_2(\Pi_2 + \Pi_3)$. Here A' has same degenerate subspaces as that of A, but arbitrary eigenvalues a'_j.

After the joint evolution of system and ancilla, a selective measurement of ancilla qubits is carried out. Generally in a quantum measurement the measuring device collapses to its pointer basis. In our scheme, we perform the projective measurement in the

40

computational basis after transforming the ancilla qubits onto the computational basis using a similarity transformation $U_a^\dagger$, such that

$$U_a|00\rangle = |\psi_0\rangle, U_a|01\rangle = |\psi_1\rangle,$$
$$U_a|10\rangle = |\psi_2\rangle, U_a|11\rangle = |\psi_3\rangle. \tag{3.11}$$

By substituting the explicit forms of $|\psi_j\rangle$, we obtain

$$U_a = \frac{1}{2} \begin{bmatrix} z^3 & z^{-1} & z^{-3} & z \\ z^9 & z^{-3} & z^{-9} & z^3 \\ z^{-9} & z^3 & z^9 & z^{-3} \\ z^{-3} & z & z^3 & z^{-1} \end{bmatrix}, \tag{3.12}$$

where $z = \exp(i\pi/8)$.

Finally, the ancilla is traced-out and the state of system qubits is characterized with the help of quantum state tomography.

According to the Lüders state update rule, if a degenerate observable A (as in Eq. (3.2)) is measured on a system in state ρ_0, then the postmeasurement state of the ensemble is described by

$$\rho_L = \sum_{l=\pm 1} \mathbb{P}_l \rho_0 \mathbb{P}_l, \tag{3.13}$$

where $\mathbb{P}_{+1} = \Pi_0 + \Pi_1$, $\mathbb{P}_{-1} = \Pi_2 + \Pi_3$. For the initial state $\rho_0 = |\Phi_0\rangle\langle\Phi_0|$, we obtain

$$\rho_L = (\mathbb{1}_4 + \mathbb{1}_2 \otimes \sigma_x)/4. \tag{3.14}$$

However according to von Neumann's degeneracy breaking state update rule, the post-

measurement state of the ensemble is given by

$$\rho_N = \sum_{j=0}^{3} \Pi_j \rho_0 \Pi_j, \tag{3.15}$$

where, Π_j's are fixed by the refining observable A'. Therefore, for the initial state $\rho_0 = |\Phi_0\rangle\langle\Phi_0|$ and the observable A' (Eq. (3.4)), the postmeasurement state collapses to a maximally mixed state, i.e.,

$$\rho_N = \mathbb{1}_4/4. \tag{3.16}$$

In both the cases, the probabilities of obtaining the eigenvalues ± 1 are identical, i.e.,

$$
\begin{aligned}
p_{+1} &= \text{Tr}(\mathbb{P}_{+1}\rho_0\mathbb{P}_{+1}) = \sum_{j=0,1} \text{Tr}(\Pi_j\rho_0\Pi_j) \quad \text{and,} \\
p_{-1} &= \text{Tr}(\mathbb{P}_{-1}\rho_0\mathbb{P}_{-1}) = \sum_{j=2,3} \text{Tr}(\Pi_j\rho_0\Pi_j).
\end{aligned} \tag{3.17}
$$

Thus although, the measurement outcomes (eigenvalues) and their probabilities are identical, the postmeasurement states ρ_L and ρ_N are different [LÖ6, vN55, HSM12, BE14]. In fact, the Uhlmann fidelity between ρ_L and ρ_N turns out to be $F(\rho_L, \rho_N) = \text{Tr}\sqrt{\sqrt{\rho_N}\rho_L\sqrt{\rho_N}} = 1/\sqrt{2}$ [NC10]. Therefore, it is possible to discriminate between the Lüders and von Neumann devices by simply characterizing the final state of the system as shown by the circuit in Fig. 3.4.

3.4 Experiment

We utilize the four spin-1/2 nuclei of 1,2-dibromo-3,5-difluorobenzene (DBDF) as our quantum register. About 12 mg of DBDF was partially oriented in 600 μl of liquid crystal

H$_1$	H$_2$	F$_3$	F$_4$	Hz		T$_2$* (s)
-37.7	2.8, 72.5	1.8, 550.0	8.3, 447.0	H$_1$		0.87
	0.0	9.2, 53.5	9, 307.0	H$_2$		0.87
		3262.2	7.6, 84.0	F$_3$		0.55
			-3262.2	F$_4$		0.55

Fig. 3.5: Molecular structure of 1,2-Dibromo-3,5-difluorobenzene, Hamiltonian parameters, and the relaxation parameters. In the table, the diagonal values indicate resonance offsets ($\omega_j/2\pi$); off-diagonal values (J_{ij}, D_{ij}) indicate the indirect and the residual direct spin-spin coupling constants respectively (in Hz); the last column lists approximate effective transverse relaxation time constants (T_2^*).

MBBA. The molecular structure of DBDF and its NMR Hamiltonian parameters are shown in Fig. 3.5. The experiments were performed at 300 K on a 500 MHz Bruker Ultra-shield NMR spectrometer.

The secular part of the spin-Hamiltonian is of the form [Cav96],

$$\mathcal{H}_0 = -\sum_{j=1}^{4}\omega_j I_{jz} + 2\pi\sum_{j,k>j}(J_{jk}+2D_{jk})I_{jz}I_{kz}$$
$$+2\pi(J_{12}-D_{12})(I_{1x}I_{2x}+I_{1y}I_{2y}), \tag{3.18}$$

where ω_j, J_{ij}, and D_{ij} are the resonance off-sets, indirect scalar coupling constants, and direct dipole-dipole coupling constants (Fig. 3.5). The strong-coupling term (i.e., the last term) is relevant only for (H$_1$, H$_2$) spins since $|\omega_1 - \omega_2| < 2\pi|D_{12}|$. We choose H$_1$, H$_2$ as ancilla (qubits 1, 2) and F$_3$, F$_4$ as the system (qubits 3, 4).

The NMR pulse diagram to implement the quantum circuit in Fig. 3.4(a) is shown in

Fig. 3.4(b). It begins with the initial state preparation. The thermal equilibrium state of the NMR system in the Zeeman eigenbasis under high-field, high-temperature, and secular approximation is given by [Lev08, Cav96],

$$\rho_{\text{eq}} = \mathbb{1}_{16}/16 + \sum_{j=1}^{4} \epsilon_j I_{zj}, \tag{3.19}$$

where $\epsilon_j \sim 10^{-5}$ are the purity factors and the second term in the right hand side corresponds to the traceless deviation density matrix. The identity part is invariant under the unitary transformations and does not give rise to observable signal. Therefore only the deviation part is generally considered for both state preparation and characterization [CPH98].

The initial state of the quantum register assumed in the theory section, i.e., $|\Phi_0\rangle$ can be prepared by applying an Hadamard operator on each of the four qubits in a pure $|0\rangle$ state. However, in NMR, the preparation of such pure states is difficult and instead a pseudopure state is used [CPH98]. In our work, we utilize a technique based on preparing a pair of pseudopure states (POPS) [Fun01]. It involves inverting a single transition and subtracting the resulting spectrum from that of the thermal equilibrium. By inverting the transition $|0000\rangle$ to $|0001\rangle$ transition using a transition selective π pulse, followed by Hadamard gates (H) on all the spins we obtain the POPS deviation density matrix:

$$\rho_{\text{POPS}} = \big(|+++ +\rangle\langle + + + +| - |+ + + -\rangle\langle + + + -|\big).$$

We then implemented the quantum circuit shown in Fig. 3.4 (a) using the pulse sequence in Fig. 3.4 (b). As evident from circuit in Fig. 3.4, controls are designed to implement U_{int} (Eq. (3.10)) since we intend to measure A. Whether to map it to A' or not is left to the device. The unitary operators U_{int} and $U_a^\dagger$ were realized by bang-bang optimal

control [BAM16]. Hadamard and tomography operations were only few hundred micro seconds long and had a simulated fidelity of about 0.99, when averaged over $\pm 10\%$ inhomogeneous RF fields. The combined operation of U_{int} and $U_a^\dagger$ was about 17 ms in duration and had an average fidelity over 0.933.

The intermediate measurement on ancilla was realized by applying strong pulse-field-gradients (PFG). By applying a π_x pulse on the system spins in between two symmetrically spaced PFG pulses, we realize the selective dephasing of the ancilla spins (Fig. 3.4 (b)). The central π_x also refocuses all the system-ancilla coherent evolutions during the ancilla measurement. When averaged over the sample volume this process retains only the diagonal terms in the density matrix of the ancilla spins and thus simulates a projective measurement of ancilla. Setting the total duration of this process to $1/(J_{34} + 2D_{34})$ also ensures refocusing of (F_3, F_4) interactions.

Finally, the density matrix of the system qubits was characterized using quantum state tomography. It involved nine independent measurements with different tomography pulses (T) (Fig. 3.4 (b)) [CGKL98, RM10].

The results of the quantum circuit (Fig. 3.4) on $|{+}{+}{+}{+}\rangle\langle{+}{+}{+}{+}|$ state by Lüders and von Neumann devices are described in Eqs. (3.14) and (3.16) respectively. For Lüders measurement with the POPS input state $|{+}{+}{+}{+}\rangle\langle{+}{+}{+}{+}| - |{+}{+}{+}{-}\rangle\langle{+}{+}{+}{-}|$, the final deviation density matrix (in circuit 3.4) is expected to be

$$\rho'_L = \mathbb{1}_2 \otimes \sigma_x/2. \tag{3.20}$$

On the other hand, for von Neumann measurement, the POPS input state leads to a maximally mixed final state with a null deviation density matrix (ρ'_N).

Fig. 3.6 compares the experimental results with the theoretically expected deviation
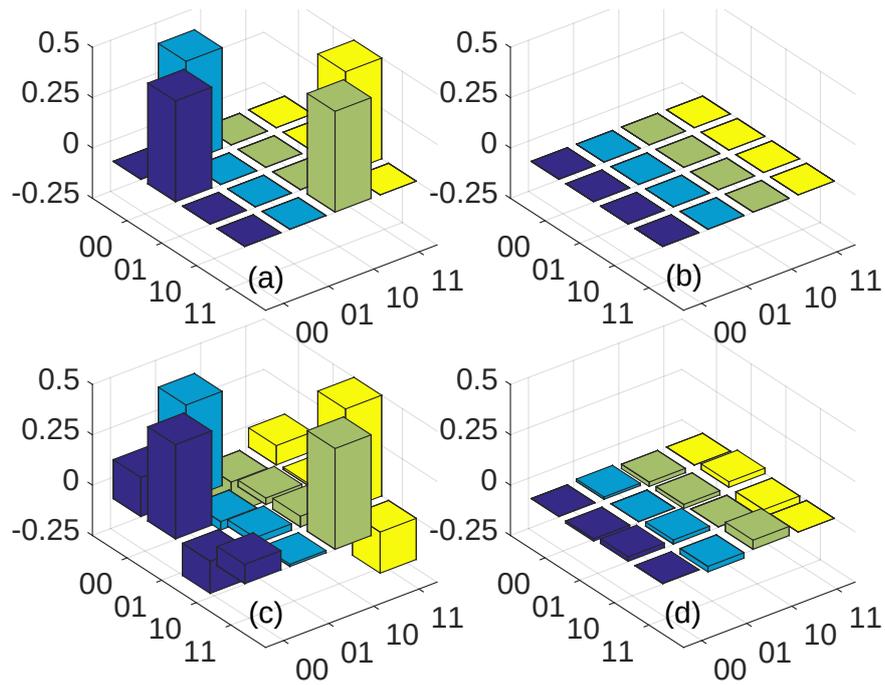
Fig. 3.6: Real (a) and imaginary (b) parts of the theoretically expected deviation density matrix for a Lüders device (ρ'_L); real (c) and imaginary (d) parts of the experimental deviation density matrix (ρ'_{exp}).

density matrices. The correlation [FPB$^+$02]

$$C = \frac{\text{Tr}[\rho'_L \rho'_{\text{exp}}]}{\sqrt{\text{Tr}[\rho'^2_L]\text{Tr}[\rho'^2_{\text{exp}}]}} \qquad (3.21)$$

between the theoretical (ρ'_L, Eq. (3.20)) and the experimental (ρ'_{exp}) deviation density matrices was 0.923. The reduction in the correlation is mainly due to coherent errors caused by imperfect unitary operators, fluctuations in the dipolar coupling constants due to temperature gradients over the sample volume, inhomogeneous RF fields, as well as due to decoherence.

The correlation expression in Eq. (3.21) is not directly applicable for the null-matrix ρ'_N. Therefore, we replace ρ'_N with random traceless diagonal matrices, and obtained 0.28 as the upper bound for the correlation of ρ'_{exp} with ρ'_N. Therefore we conclude that the experimental deviation density matrix is much closer to ρ'_L (Eq. (3.20)), and strongly favors the Lüders update rule.

3.5 Conclusions

Quantum measurements, involving probabilistic state collapse and corresponding measurement outcomes, has always been mysterious. There have been attempts to deduce rules based on phenomenological observations. According to one of the earliest reduction rules, given by von Neumann, superposition in a degenerate subspace is destroyed by the measurement of the respective degenerate observable. This rule was later substantially modified by Gerhart Lüders. The modified rule, which is most commonly used, implies that superpositions within the degenerate subspaces are preserved under such a measurement.

A protocol to determine whether a given measuring device is Lüders or von Neumann was

recently formulated by Hegerfeldt and Mayato [HSM12]. In this work, we have adapted this protocol for quantum information systems, and utilize ancilla qubits for performing a desired measurement on system qubits. Moreover, we describe an NMR experiment, with two system qubits and two ancilla qubits, to discriminate between Lüders and von Neumann devices. Within the limitations of experimental NMR techniques, we found that the measurements are of Lüders type.

There is a possibility that the above measurement is still of von Neumann type, if the chosen initial state happens to be a nondegenerate eigenstate of the actual system observable (A'). One way to rule out this possibility is by changing the initial state (Fig. 3.2). However, it is also possible that the actual system observable is dynamic, in which case it is even more difficult to discriminate between Lüders and von Neumann measurements. In this work we have not excluded these possibilities. Nevertheless, the present work opens many interesting questions. For example, how can we build a von Neumann measuring device, or even an intermediate measuring device that partly breaks the degeneracy? More importantly, further research in this direction may throw some light on fundamental aspects of quantum measurement itself.

Chapter 4

Ancilla induced amplification of quantum Fisher information

"Fisher information as a 'mother' information."-B.R.Frieden [Fri99]

4.1   Abstract

Given a quantum state with an unknown parameter being measured with a suitable observable, Quantum Fisher Information (QFI) is a measure of the amount of information that one can extract about the unknown parameter. QFI also quantifies the maximum achievable precision in estimating the unknown parameter with a given amount of resource via quantum Cramer-Rao bound. In this work, we describe a protocol to amplify QFI of a single target qubit precorrelated with a set of ancillary qubits. Using an NMR system as an example, we show that a single quadrature NMR signal of only ancillary qubits suffices to perform the quantum state tomography (QST) of target qubit's deviation part of the density matrix. We experimentally demonstrate this protocol using a star-topology spin-system consisting of a ^{13}C nuclear spin as the target qubit and three ^{1}H nuclear spins as ancillary qubits. We prepare the target qubit in various initial states, perform experimental QST, and estimate the amplification of QFI in each case. We also show that, at a high-temperature scenario like in the case of NMR, the QFI-amplification scales linearly with the number of ancillary qubits and quadratically with the Bloch radius [SKM18].

4.2   Introduction

Quantum devices are expected to bring out a revolution in the way information is stored, manipulated, and communicated [NC10]. An important criterion to achieve this goal is the capability to efficiently measure two-level quantum systems, or qubits [DiV]. Spin-based systems are among various architectures which are being pursued for the physical realization of a quantum processor [LJL+10]. Nuclear spins in favorable atomic or molecular systems have the capability to store quantum information for sufficiently long duration and to allow precise implementation of desired quantum dynamics. Accordingly, Nuclear Magnetic Resonance (NMR) is often considered as a convenient testbed for quantum emulations [CFH97, CPH98, CLK+00]. In a conventional NMR scheme, tiny nuclear polarizations demand a collective ensemble measurement of about 10^{15} identical spin-systems. There have been several proposals to increase the sensitivity of nuclear spin detection. For example, dynamic nuclear polarization (DNP) transfers polarization from electrons to nuclei, thereby enhancing the nuclear polarization up to three orders of magnitude [MDB+08]. Optical polarization and detection often enables single-spin measurements, such as in the case of nitrogen vacancy centers in diamond [WGFVB97]. Further improvements in sensitivity are possible by using quantum metrology which has recently attracted significant research interests [TA14]. Cappellaro et. al. have proposed a metrology scheme by measuring a set of ancillary qubits after correlating them with the target qubit [CEB+05]. N-spin quantum metrology in the presence of decoherence has been discussed by Knysh et. al. [KCD]. Quantum metrology in a solid state NMR system exploiting spin-diffusion has been proposed by Negoro et. al. [NTKK11].

The present work involves a single target qubit and a set of ancillary qubits. While the methods described in the following can be suitably adopted for a quantum register

with a general topology, we particularly focus on star-topology registers (STRs). An STR consists of a central target qubit uniformly interacting with a set of identical ancillary qubits which have no effective interaction among themselves (see figs. 4.1(a) and (b)). Recently STRs have been utilized for several interesting applications. The main advantage of an STR is that it allows simultaneous implementation of C-NOT operations on the ancillary qubits controlled by the target qubit without requiring individual control of ancillary qubits. Simmons et. al. exploited this property to prepare large NOON states and used them to sense ultra-low magnetic fields [SJK+10]. Abhishek et. al. proposed efficient measurement of translational diffusion in liquid ensembles of STR molecules [SSM14]. Using a 37-qubit STR, Varad et. al. demonstrated a strong algorithmic cooling of the target qubit by repeatedly releasing its entropy to ancillary qubits [PBKM17]. Deepak et. al. transferred the large polarization of ancillary qubits directly to the long-lived singlet-state of a central pair of qubits in an STR-like register [KM17]. More recently, Soham et. al. have utilized STRs to investigate the rigidity of temporal order in periodically driven systems [PNMS18].

In this work, we propose and experimentally demonstrate a protocol to perform quantum state tomography (QST) of a target qubit in an STR. We find that a single-scan quadrature NMR signal of ancillary qubits of an STR precorrelated with the central target qubit is sufficient to tomograph the target qubit's deviation part of the density matrix. Moreover, this procedure leads to a strong amplification of Quantum Fisher Information (QFI). QFI quantifies the amount of information that one can extract, by measuring a given observable, about an unknown parameter corresponding to a quantum state [TA14]. Moreover, QFI allows one to estimate the quantum Cramer-Rao bound, which sets an upper-bound for the maximum achievable precision in estimating an unknown parameter with a given amount of resource [KDD13]. Here we also find that, at low quantum state purities, QFI scales linearly with the number of ancillary

qubits and quadratically with the Bloch radius.

In sec. 4.3.1 we describe QST of the target qubit without using ancillary qubits. In sec. 4.3.2 we describe QST of the target qubit after precorrelating it with ancillary qubits. In sec. 4.3.3 we describe NMR aspects of QST and present the experimental results. In sec. 4.4 we estimate the QFI of a single uncorrelated qubit as well as that of a target qubit precorrelated with certain ancillary qubits in an STR using analytical or numerical techniques. Finally we summarize and conclude in sec. 4.5.

4.3 QST of a single target qubit

4.3.1 QST of a target qubit without ancilla

Consider a single target qubit in a mixed state with Bloch radius $\varepsilon_{t,1} \in [0,1]$. In the Bloch sphere, we can represent it as a convex sum of the maximally mixed state $\mathbb{1}_2/2$ and a pure state $|\psi_{\theta_0,\phi_0}\rangle\langle\psi_{\theta_0,\phi_0}|$, where

$$|\psi_{\theta_0,\phi_0}\rangle = \cos(\theta_0/2)|0\rangle + e^{i\phi_0}\sin(\theta_0/2)|1\rangle. \tag{4.1}$$

The corresponding density matrix is

$$
\begin{aligned}
\varrho_{\theta_0,\phi_0} &= (1-\varepsilon_{t,1})\mathbb{1}_2/2 + \varepsilon_{t,1}|\psi_{\theta_0,\phi_0}\rangle\langle\psi_{\theta_0,\phi_0}| \\
&= \frac{1}{2}\begin{bmatrix} 1 + \varepsilon_{t,1}\cos\theta_0 & \varepsilon_{t,1}e^{-i\phi_0}\sin\theta_0 \\ \varepsilon_{t,1}e^{i\phi_0}\sin\theta_0 & 1 - \varepsilon_{t,1}\cos\theta_0 \end{bmatrix}, \\
&= \mathbb{1}_2/2 + \varepsilon_{t,1}\sigma_{\theta_0,\phi_0}/2, \tag{4.2}
\end{aligned}
$$

where the traceless deviation part

$$\sigma_{\theta_0,\phi_0} = \sin\theta_0 \cos\phi_0 \ \sigma_x + \sin\theta_0 \sin\phi_0 \ \sigma_y + \cos\theta_0 \ \sigma_z = \hat{n}_0.\vec{\sigma}. \qquad (4.3)$$

Here $\sigma_x, \sigma_y, \sigma_z$ are the Pauli matrices and $\varepsilon_{t,1}\hat{n}_0$ is the Bloch vector. Now we describe an NMR protocol to perform the single-qubit QST. The uniform background represented by the identity in eq. (4.2) does not lead to any NMR signal and hence is generally ignored during QST [NC10]. The second-term in eq. (4.2) is the trace-less part and is referred to as the deviation part of the density matrix. After applying suitable readout pulse, the deviation part gives raise to an NMR signal. An NMR signal is recorded as a collective emf induced by the spin ensemble precessing in the Zeeman field. Modern spectrometers are equipped with the quadrature detection scheme which involves reading of two orthogonal magnetization components simultaneously and independently [Lev08]. In other words, the quadrature detection allows the reading $\langle I_x \rangle + i\langle I_y \rangle$, where $I_{x/y} = (\sigma_{x/y})/2$ are the components of spin-angular momentum operators.

As illustrated in fig. 4.1(c), QST of the single spin can be achieved using two independent experiments [SRM13]: (i) estimating $\phi_0 = \tan^{-1}(\langle I_y \rangle/\langle I_x \rangle)$ via a quadrature measurement of $\langle I_x \rangle + i\langle I_y \rangle$; (ii) estimating θ_0 via $\langle I_z \rangle$ measurement using a read-out pulse after dephasing the off-diagonal terms using a pulsed field gradient (PFG). The correlation [FPB$^+$02] between the expected (σ_{θ_0,ϕ_0}), and the experimental ($\tilde{\sigma}_{\theta_0,\phi_0}$) deviation density matrices is calculated using

$$C = \frac{\mathrm{Tr}[\tilde{\sigma}_{\theta_0,\phi_0}\sigma_{\theta_0,\phi_0}]}{\sqrt{\mathrm{Tr}[\tilde{\sigma}^2_{\theta_0,\phi_0}]\mathrm{Tr}[\sigma^2_{\theta_0,\phi_0}]}}. \qquad (4.4)$$
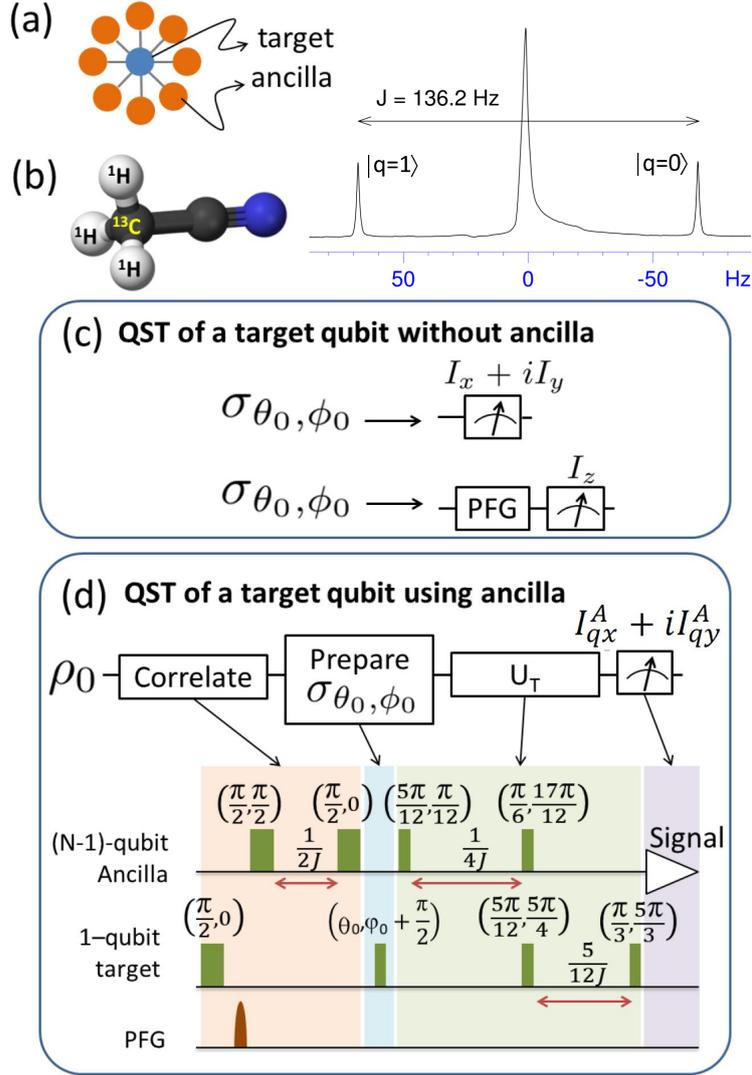
Fig. 4.1: (a) Schematic representation of an STR, (b) molecular structure of acetonitrile corresponding to a 4-qubit STR and ^{1}H spectrum showing the two satellite transitions corresponding to the two Zeeman basis states of ^{13}C (the central peak is suppressed as explained in the text) (c) QST of a target qubit without ancilla, requiring two independent NMR experiments, (d) QST of a target qubit using three ancillary qubits, requiring a single quadrature detection of ancillary qubits without decoupling the target during acquisition. In (d), each RF pulse shown by a rectangle is labeled with two parameters - nutation angle and phase respectively (see Appendix 8.3). The tomography parameters are optimized using a genetic algorithm subject to certain constraints such as rank, condition number, and overall signal enhancement [SRM13].

4.3.2 QST of a target qubit in an STR

Here we consider an N-qubit STR consisting of a single target qubit surrounded by a set of $N-1$ indistinguishable ancillary qubits (fig. 4.1(a)). Under the weak-coupling approximation, Hamiltonian for the STR is of the form

$$H = \hbar\omega_t I_{1z} + \hbar\omega_a \sum_{j=2}^{N} I_{jz} + \pi\hbar J \sum_{j=2}^{N} 2I_{1z}I_{jz}, \tag{4.5}$$

where $\omega_t = -\gamma_t B_0(1+\delta_t)$ and $\omega_a = -\gamma_a B_0(1+\delta_a)$ are the Larmor precession frequencies of the target and ancilla respectively, $\gamma_{t/a}$ are gyromagnetic ratios, $\delta_{t/a}$ are chemical shifts, B_0 is the strong external magnetic field strength, and $I_{jz} = \mathbb{1}_{2^{j-1}} \otimes \frac{\sigma_z}{2} \otimes \mathbb{1}_{2^{N-j}}$ is the spin angular momentum operator corresponding to the jth qubit [Lev08]. Because of the magnetic-equivalence symmetry, the scalar couplings between the target and indistinguishable ancillary qubits are all same, and of magnitude J, while those among the ancillary qubits become unobservable and ineffective (fig. 4.1 (a) and (b)). In the following we describe (i) precorrelating a target qubit with ancillary qubits, (ii) implementing an arbitrary transformation on the target qubit, and (iii) QST of the target qubit's deviation part of the density matrix by a single-shot quadrature measurement of ancillary qubits (fig. 4.1(d)).

(i) In a strong Zeeman field B_0, the thermal equilibrium state of STR is,

$$\begin{aligned}
\rho_0 &= \frac{e^{-H/(k_B T)}}{\text{Tr}[e^{-H/(k_B T)}]} \\
&\approx \mathbb{1}_{2^N}/2^N + \varepsilon_{t,N} I_{1z} + \varepsilon_{a,N} \sum_{i=2}^{N} I_{iz}
\end{aligned} \tag{4.6}$$

where the latter form is known as the high-temperature and high field approximation

[Cav96, Lev08] with

$$\varepsilon_{t,N} = \frac{\hbar\gamma_t B_0}{2^N k_B T} \quad \text{and} \quad \varepsilon_{a,N} = \frac{\hbar\gamma_a B_0}{2^N k_B T} \tag{4.7}$$

are the generalized Bloch radii (each $\lesssim 10^{-5}$) [ZSM$^+$13]. Here k_B is the Boltzmann constant and T is the absolute temperature. Thus the thermal state is practically an uncorrelated state. Quantum correlations can enhance precision in estimating an unknown parameter. For example, in an ensemble of k non-interacting qubits, square of the error in estimating the parameter, say, θ goes as $1/k$ i.e., $(\Delta\theta)^2 \sim 1/k$ (shot-noise scaling) [TA14]. However if the qubits are interacting, then we can exploit the entanglement between them to achieve Heisenberg scaling i.e., $(\Delta\theta)^2 \sim 1/k^2$ [TA14]. Motivated by this fact, here we utilize the standard NMR technique, namely INEPT [Cav96] to prepare a correlated state of the form

$$\rho_1 = \mathbb{1}_{2^N}/2^N + \varepsilon_{a,N} 2I_{1z} \sum_{i=2}^{N} I_{iz}. \tag{4.8}$$

We are going to show that this leads to a linear amplification in QFI, and hence we can achieve better precision in estimating an unknown parameter. The corresponding pulse sequence is shown in fig. 4.1(d). For a large STR with $\varepsilon_{a,N} > \varepsilon_{t,N}$, the above state corresponds to a large anti-phase spin-order and accordingly leads to a strong NMR signal after applying a suitable read-out pulse.

(ii) The target is now ready for an arbitrary local transformation

$$\rho_1$$

$$\downarrow \quad e^{-i\theta_0\{\cos(\phi_0+\pi/2)I_{1x}+\sin(\phi_0+\pi/2)I_{1y}\}}$$

$$\rho_{\theta_0,\phi_0} = \mathbb{1}_{2^N}/2^N + \varepsilon_{a,N}\left(\sigma_{\theta_0,\phi_0} \otimes \mathbb{1}_{2^{N-1}}\right) \sum_{i=2}^{N} I_{iz}. \tag{4.9}$$

(iii) The problem we consider now is: If STR is originally prepared in the state described in eq. (4.9) without revealing θ_0 and ϕ_0, can we perform the QST with only a single quadrature NMR signal of the ancillary qubits to extract the unknown parameters θ_0 and ϕ_0?

The answer is affirmative, and to this end, we first apply the QST pulses (U_T) as shown in fig. 4.1(d) and read the signal from ancillary qubits. In general, we obtain two spectral lines from the ancillary qubits corresponding to $|q=0\rangle$ and $|q=1\rangle$ Zeeman basis states of the target qubit (fig. 4.1(b)). We denote the observables corresponding to the ancilla magnetization along $\alpha \in \{x, y\}$ directions conditional to the target qubit's basis states as

$$I_{q\alpha}^A = \left[(|q\rangle\langle q| \otimes \mathbb{1}_{2^{N-1}}) \sum_{j=2}^{N} I_{j\alpha} \right]. \tag{4.10}$$

Following Abhishek et. al. [SRM13], we first setup the 4×3 dimensional constraint matrix Z with elements

$$Z_{1j} = \text{Tr}(B_j I_{0x}^A), \qquad Z_{2j} = \text{Tr}(B_j I_{0y}^A),$$
$$Z_{3j} = \text{Tr}(B_j I_{1x}^A), \qquad Z_{4j} = \text{Tr}(B_j I_{1y}^A), \tag{4.11}$$

where $B_j = \sum_{i=2}^{N} U_T 2 I_{1\alpha_j} I_{iz} U_T^\dagger$ and $\alpha_1 = x$, $\alpha_2 = y$, $\alpha_3 = z$, and U_T is the QST propagator (see fig. 4.1(d) and Appendix 8.3). While the tomography sequence U_T is not unique, the pulse-sequence in fig. 4.1(d) was obtained after numerically maximizing the column-wise norm of the constraint matrix Z while simultaneously minimizing its overall condition number (Appendix 8.4). Maximizing the column-wise norm is to uniformly maximize the weights corresponding to all α_j. The condition number is a measure of invertibility of the constraint matrix Z. Lower the condition number, higher is the precision in determining the unknowns in the presence of noise [BKW05], [AMHR13].

The tomography problem then reduces to solving the following set of independent linear constraint equations,

$$
Z \begin{bmatrix} \sin\theta_0 \cos\phi_0 \\ \sin\theta_0 \sin\phi_0 \\ \cos\theta_0 \end{bmatrix} = \begin{bmatrix} \langle I_{0x}^A \rangle \\ \langle I_{0y}^A \rangle \\ \langle I_{1x}^A \rangle \\ \langle I_{1y}^A \rangle \end{bmatrix}, \tag{4.12}
$$

where elements of the right hand side correspond to intensities of NMR signal. Thus, a single-shot quadrature read-out of ancillary qubits provides four real constraints sufficient to determine the two unknowns θ_0 and ϕ_0, and hence achieve QST of the target qubit [SRM13]. In addition, as we are going to show in sec. 4.4, we achieve at least 6 times amplification of QFI in this process.

4.3.3 Experiments

The experiments were carried out on a Bruker 500 MHz high-resolution NMR spectrometer using a liquid sample containing 300 µl of acetonitrile (H_3C_2N) dissolved in 400 µl of deuterated acetonitrile (D_3C_2N) at 300 K. We used the spin-1/2 nuclei of naturally abundant ^{13}C nucleus as the target qubit and three spin-1/2 hydrogen nuclei of the methyl group as ancillary qubits (qubits 2, 3, and 4) (see fig. 4.1(b)). The ^1H NMR spectrum of acetonitrile shown in fig. 4.1(b) displays two satellite peaks corresponding to the two Zeeman basis states of ^{13}C (abundance 1.1 %). Here the central peak arising from ^1H spins of ^{12}C molecules (abundance 98.9 %) is suppressed by using an initial transition-selective 90 degree pulse followed by a PFG. In this spin-system, the indirect spin-spin C-H couplings are $J_{1i} = 136.2$ Hz ($i = 2, 3, 4$) while the H-H couplings are ineffective due to magnetic equivalence [Lev08]. We had chosen on-resonance carrier

frequencies for both the nuclear species. Experimental steps for preparing correlated STR, transformation of the target qubit into σ_{θ_0,ϕ_0}, and finally applying QST pulses (U_T) and measurements are described in fig. 4.1 (d). First we prepared a target-ancilla correlated state of the form ρ_1 (eq. (4.8)). Then using a rotation by θ_0 about a unit vector $\cos(\phi_0 + \pi/2)\hat{x} + \sin(\phi_0 + \pi/2)\hat{y}$ we rotate the target state $\sigma_{0,0}$ into σ_{θ_0,ϕ_0} (see eq. (4.9)). We have arbitrarily chosen five distinct states of the target qubit and for each of them we experimentally performed QST using a single quadrature NMR signal of ancillary qubits as explained in sec. 4.3.2. High correlations C (eq. (4.4)) obtained for various states tabulated in Table 4.1 indicate highly robust QST performance.

σ_{θ_0,ϕ_0}	C
σ_{0,ϕ_0}	0.994
$\sigma_{\pi/2,0}$	0.984
$\sigma_{\pi/2,\pi/2}$	0.998
$\sigma_{\pi/4,0}$	0.999
$\sigma_{\pi/4,\pi/2}$	0.999

Table 4.1: Experimental Correlations C for various unknown states.

4.4 Estimation of QFI in an STR

Consider a quantum system prepared in a state in the neighborhood of ρ_{θ_0,ϕ_0} and M be a given observable with spectral decomposition $M = \sum_i m_i |m_i\rangle\langle m_i|$. Let us first assume that the polar angle θ has a distribution around θ_0, while ϕ_0 is precisely known. Now we may calculate the probability $f_{\theta,\phi_0}(m_i) = \text{Tr}(\rho_{\theta,\phi_0}|m_i\rangle\langle m_i|)$ corresponding to the eigenvalue m_i. QFI is defined in terms of non-zero probability distributions as [TA14]

$$F_\theta(\rho_{\theta_0,\phi_0}, M) = \sum_{i,f\neq0} \frac{1}{f_{\theta_0,\phi_0}(m_i)} \left(\frac{\partial f_{\theta,\phi_0}(m_i)}{\partial \theta}\bigg|_{\theta_0} \right)^2. \tag{4.13}$$

Here $\partial f_{\theta,\phi_0}(m_i)/\partial\theta|_{\theta_0}$ quantifies the sensitivity of the observable M to small fluctuations in θ around θ_0. Similarly, if the polar angle is held fixed at θ_0, while distributing azimuthal angle ϕ around ϕ_0, QFI is then given by

$$F_\phi(\rho_{\theta_0,\phi_0}, M) = \sum_{i,f\neq 0} \frac{1}{f_{\theta_0,\phi_0}(m_i)} \left(\left. \frac{\partial f_{\theta_0,\phi}(m_i)}{\partial\phi} \right|_{\phi_0} \right)^2. \tag{4.14}$$

In the following we consider the specific cases of a single-qubit and an N-qubit STR and estimate the QFI corresponding to polar, azimuthal, and dual-parameters.

4.4.1 QFI of a single-qubit

Consider a single target qubit prepared in the state

$$\varrho_{\theta,\phi_0} = \mathbb{1}_2/2 + \varepsilon_{t,1}\sigma_{\theta,\phi_0}/2, \tag{4.15}$$

where θ is in the neighborhood of θ_0 (see eq. (4.2)).

Since QFI depends on the observable M, it is natural to ask which observable maximizes QFI. Such an optimal observable that maximizes QFI is known as the unbiased observable $M_{\overleftrightarrow{\theta_0},\phi_0}$ and it satisfies the flow equation

$$\left. \frac{\partial\varrho_{\theta,\phi_0}}{\partial\theta} \right|_{\theta_0} = \frac{1}{2}\left(M_{\overleftrightarrow{\theta_0}\phi_0}\varrho_{\theta_0,\phi_0} + \varrho_{\theta_0,\phi_0}M_{\overleftrightarrow{\theta_0}\phi_0} \right) \tag{4.16}$$

[KDD13]. The solution of this equation leads to the unbiased observable in the form of

a symmetric logarithmic derivative (SLD),

$$
M_{\overleftrightarrow{\theta_0},\phi_0} = \sum_{i,j,\lambda_i+\lambda_j\neq 0} \frac{2\left\langle \lambda_i \left| \frac{\partial \varrho_{\theta,\phi_0}}{\partial \theta}\right|_{\theta_0} \right| \lambda_j \right\rangle}{\lambda_i + \lambda_j} |\lambda_i\rangle\langle\lambda_j|, \tag{4.17}
$$

$$
= \varepsilon_{t,1} \left. \frac{\partial \hat{n}}{\partial \theta}\right|_{\theta_0} .\vec{\sigma} \tag{4.18}
$$

where λ_i and $|\lambda_i\rangle$ are the eigenvalues and eigenvectors respectively of $\varrho_{\theta_0,\phi_0}$ (see [KDD13] and Appendix 8.5.1). Since $\hat{n}_0. \left.\frac{\partial \hat{n}}{\partial \theta}\right|_{\theta_0} = 0$, the unbiased observable corresponds to a direction orthogonal to the target state $\varrho_{\theta_0,\phi_0}$ [TA14].

For the optimal case, we obtain the upper bound for the mixed state QFI (see Appendix 8.5.1),

$$
F_\theta(\varrho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0}) = \varepsilon_{t,1}^2 = \mathrm{Tr}\left[\varrho_{\theta_0,\phi_0}\left(M_{\overleftrightarrow{\theta_0},\phi_0}\right)^2\right], \tag{4.19}
$$

since $\left(M_{\overleftrightarrow{\theta_0},\phi_0}\right)^2 = \varepsilon_{t,1}^2 \mathbb{1}_2$ [ZSM$^+$13].

As a specific example, for the state $\rho_{0,0} = |0\rangle\langle 0|$, we obtain $M_{\overleftrightarrow{0},0} = \sigma_x$ as the unbiased observable, and the maximum QFI, $F_\theta(\rho_{0,0}, \sigma_x) = 1$.

An important application of QFI is that it provides a bound to the variance $(\Delta\theta)^2$, via quantum Cramer-Rao bound

$$
(\Delta\theta)^2 \geq \frac{1}{kF_\theta(\varrho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0})} = \frac{1}{k\varepsilon_{t,1}^2}, \tag{4.20}
$$

where k is the number of independent measurements on identically prepared states in the neighborhood of $\varrho_{\theta_0,\phi_0}$ [KDD13]. In the NMR case, the number of independent measurements $k \sim 10^{15}$, same as the number of molecules in the experimental sample. Taking $\varepsilon_{t,1} \sim 10^{-5}$, we obtain $F_\theta \sim 10^{-10}$. Nevertheless, $\Delta\theta < 10^{-2}$ radians, which

represents a reasonably high precision. In practice however, the precision is also limited by the experimental errors such as mis-calibrations, incoherence and decoherence.

Similarly, for the azimuthal parameter we obtain SLD

$$M_{\theta_0,\overleftrightarrow{\phi_0}} = 2 \left. \frac{\partial \varrho_{\theta_0,\phi}}{\partial \phi} \right|_{\phi_0} = \varepsilon_{t,1} \left. \frac{\partial \hat{n}}{\partial \phi} \right|_{\phi_0} . \vec{\sigma}. \tag{4.21}$$

Since $\hat{n}_0 . \left. \frac{\partial \hat{n}}{\partial \phi} \right|_{\phi_0} = 0$, to achieve optimal measurement one has to measure in a direction orthogonal to the state $\varrho_{\theta_0,\phi_0}$. With unbiased observable (SLD) we obtain (see Appendix 8.5.2),

$$F_\phi(\varrho_{\theta_0,\phi_0}, M_{\theta_0,\overleftrightarrow{\phi_0}}) = \varepsilon_{t,1}^2 \sin^2 \theta_0 = \text{Tr}\left[\varrho_{\theta_0,\phi_0} \left(M_{\theta_0,\overleftrightarrow{\phi_0}} \right)^2 \right] \tag{4.22}$$

[ZSM+13]. The quantum Cramer-Rao bound in this case is therefore

$$(\Delta\phi)^2 \geq \frac{1}{k F_\phi(\varrho_{\theta_0,\phi_0}, M_{\theta_0,\overleftrightarrow{\phi_0}})} = \frac{1}{k \varepsilon_{t,1}^2 \sin^2 \theta_0}. \tag{4.23}$$

We now seek an effective dual parameter QFI, denoted by $\mathbb{F}(\varrho_{\theta_0,\phi_0})$, which quantifies the maximum overall information. To this end, we utilize two-parameter quantum Cramer-Rao bound given by [YNSA17]

$$(\Delta\theta)^2 + (\Delta\phi)^2 \geq \frac{1}{(2k)\mathbb{F}(\varrho_{\theta_0,\phi_0})}, \tag{4.24}$$

where the total number of measurements is now $2k$ owing to the individual measurement of θ, ϕ (see Appendix 8.6). Here the effective dual-parameter QFI is related to the single-

parameter QFIs via

$$\frac{1}{\mathbb{F}(\varrho_{\theta_0,\phi_0})} = \frac{2}{F_\theta(\varrho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0})} + \frac{2}{F_\phi(\varrho_{\theta_0,\phi_0}, M_{\theta_0,\overleftrightarrow{\phi_0}})} = \frac{2(1 + \sin^2\theta_0)}{\varepsilon_{t,1}^2 \sin^2\theta_0}. \qquad (4.25)$$

4.4.2 QFI of an N-qubit STR

Polar parameter

Let us first consider an N-qubit STR prepared in a precorrelated initial state in the neighborhood of ρ_{θ_0,ϕ_0} described in eq. (4.9). In this case, maximum QFI corresponding to an unbiased observable $M_{\overleftrightarrow{\theta_0},\phi_0}$ (SLD) is given by (see eq. (4.19))

$$F_\theta(\rho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0}) = \mathrm{Tr}\left[\rho_{\theta_0,\phi_0}\left(M_{\overleftrightarrow{\theta_0},\phi_0}\right)^2\right] \qquad (4.26)$$

[KDD13]. Using the form of $M_{\overleftrightarrow{\theta_0},\phi_0}$ as given in eq. (4.17), we obtain

$$F_\theta(\rho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0}) = \sum_{i,j,\lambda_i+\lambda_j \neq 0} \frac{4\left|\left\langle\lambda_i\left|\frac{\partial\rho_{\theta,\phi_0}}{\partial\theta}\right|_{\theta_0}\left|\lambda_j\right\rangle\right|^2}{(\lambda_i + \lambda_j)^2}\lambda_i. \qquad (4.27)$$

In general, QFI depends on the size of STR as well as its initial purity as illustrated in Fig. 4.2 (a). For high purities, there seems to be little enhancement in QFI. On the other hand for low purities, we find empirically that the maximum QFI has the form

$$F_\theta(\rho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0}) \approx \varepsilon_{a,1}^2(N-1), \qquad (4.28)$$

where $N \geq 2$. Thus in the case of small purity, in an STR with the target qubit precorrelated with ancillary qubits, QFI grows linearly with the number of ancillary qubits
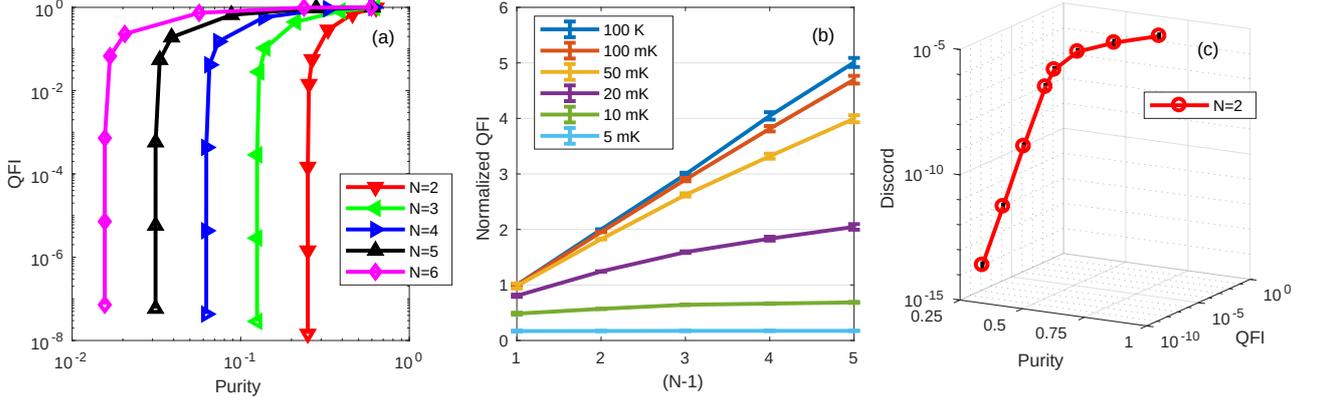
Fig. 4.2: (a) QFI $F_\theta(\rho_{\theta_0,\phi_0}, M_{\overset{\leftrightarrow}{\theta}_0,\phi_0})$ versus purity $\text{Tr}[\rho_0^2]$ at various values of N, (b) Normalized QFI $F_\theta(\rho_{\theta_0,\phi_0}, M_{\overset{\leftrightarrow}{\theta}_0,\phi_0})/\varepsilon_{a,1}^2$ versus number of ancillary spins $(N-1)$ at various bath temperature values T, and (c) discord versus purity and QFI for $N=2$.

and quadratically with the generalized Bloch radius $\varepsilon_{a,1}$. The corresponding normalized QFI plotted in Fig. 4.2 (b) shows linear dependence at high temperatures (low purities) and sublinear dependence at low temperatures (high purities). The origin of such an enhancement is interesting. It seems to emerge from quantum correlations between the central target qubit and ancillary qubits established by the precorrelation step followed by the rotation of the central qubit. To illustrate this fact, we considered the $N=2$ case, and calculated quantum discord [LMXW11, MBC+12, KRMP12] between the central qubit and the single ancillary qubit, as well as QFI at various purity values. The results are shown in Fig. 4.2 (c). As expected, both discord and QFI rapidly raise at low purities but saturate at high purities, indicating that discord might be the origin of QFI amplification. A detailed analysis of the relation between QFI and quantum discord has been carried out by Sunho Kim et. al [KLKW18]. Note that in NMR systems at room temperature, there can be no entanglement at any stage of the evolution due to low purity [BCJ+99]. However also see [LZJ+06] in this regard.

Since QFI is increasing linearly with the size of STR as in eq. (4.28), the quantum

Cramer-Rao bound for the variance $(\Delta\theta)^2$ in this case is

$$(\Delta\theta)^2 \geq \frac{1}{k\varepsilon_{a,1}^2(N-1)}. \tag{4.29}$$

It can be noted that a similar precorrelation between probe and ancillary qubits in the presence of noise also leads to the enhancement in QFI [HMM16].

However consider the uncorrelated state at a high-temperature limit,

$$\rho_{\theta_0,\phi_0}^{\text{uc}} \approx \mathbb{1}_{2^N}/2^N + \varepsilon_{t,N}(\sigma_{\theta_0,\phi_0} \otimes \mathbb{1}_{2^{N-1}})/2 + \varepsilon_{a,N}\sum_{i=2}^{N} I_{iz} \tag{4.30}$$

(see eq. (4.6)). In this case, again using the numerical approach, we found that

$$F_\theta(\rho_{\theta_0,\phi_0}^{\text{uc}}, M_{\overleftrightarrow{\theta_0},\phi_0}) \approx \varepsilon_{t,1}^2(1 + F_\theta(\rho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0})) \approx \varepsilon_{t,1}^2,$$

since $F_\theta(\rho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0}) \ll 1$ in small purity states, which is no better than the single qubit case described in eq. (4.19). Thus ancillary qubits offer no advantage unless they are precorrelated with the target. This implies that $\rho_{\theta_0,\phi_0}^{\text{uc}}$ is equivalent to $\varrho_{\theta_0,\phi_0}$ with respect to QFI.

Azimuthal parameter

Again we consider an N-qubit STR prepared in the neighborhood of a precorrelated initial state described by eq. (4.9). Using similar methods applied for obtaining eq. (4.28), we found

$$F_\phi(\rho_{\theta_0,\phi_0}, M_{\theta_0,\overleftrightarrow{\phi_0}}) \approx r\varepsilon_{a,1}^2(N-1), \tag{4.31}$$

where the factor $r \in [0, 1]$ depends on θ_0 and ϕ_0, and $N \geq 2$. The corresponding quantum Cramer-Rao bound for the variance $(\Delta\phi)^2$ is

$$(\Delta\phi)^2 \geq \frac{1}{kr\varepsilon_{a,1}^2(N-1)}. \tag{4.32}$$

However consider the uncorrelated state $\rho_{\theta_0,\phi_0}^{\mathrm{uc}}$ described in eq. (4.30). In this case, using the numerical approach we found that

$$F_\phi(\rho_{\theta_0,\phi_0}^{\mathrm{uc}}, M_{\theta_0,\overleftrightarrow{\phi_0}}) \approx \varepsilon_{t,1}^2 \sin^2\theta_0. \tag{4.33}$$

Comparing the above equation with eq. (4.22), we find no advantage of ancillary qubits unless they are precorrelated with the target and that, $\varrho_{\theta_0,\phi_0}$ and $\rho_{\theta_0,\phi_0}^{\mathrm{uc}}$ are equivalent with respect to QFI.

Dual parameters - θ and ϕ

Just like the one-qubit case (see eqs. (4.24) and (4.25)), the dual-parameter quantum Cramer-Rao bound in the N-qubit STR is given by [YNSA17]

$$(\Delta\theta)^2 + (\Delta\phi)^2 \geq \frac{1}{2k\mathbb{F}(\rho_{\theta_0,\phi_0})}, \tag{4.34}$$

where

$$\mathbb{F}(\rho_{\theta_0,\phi_0}) \approx \frac{\varepsilon_{a,1}^2(N-1)r}{2(1+r)} \tag{4.35}$$

is the effective dual-parameter QFI.

| σ_{θ_0,ϕ_0} | QFI | | | | | |
| | With QST-based observables | | | With optimal observables (SLD) | | |
	$\mathbb{F}_Q(\varrho_{\theta_0,\phi_0})/\varepsilon_{a,1}^2$ (Uncorrelated)	$\mathbb{F}_Q(\rho_{\theta_0,\phi_0})/\varepsilon_{a,1}^2$ (Correlated STR)	A	$\mathbb{F}(\varrho_{\theta_0,\phi_0})/\varepsilon_{a,1}^2$ (Uncorrelated)	$\mathbb{F}(\rho_{\theta_0,\phi_0})/\varepsilon_{a,1}^2$ (Correlated STR)	A
σ_{0,ϕ_0}	0	0	-	0	0	-
$\sigma_{\pi/2,0}$	0.008	0.049	6	0.016	0.75	47
$\sigma_{\pi/2,\pi/2}$	0.008	0.056	7	0.016	0.75	47
$\sigma_{\pi/4,0}$	0.004	0.028	7	0.010	0.5	50
$\sigma_{\pi/4,\pi/2}$	0.004	0.033	8	0.010	0.5	50

Table 4.2: Estimated QFIs for a set of states and corresponding QFI-amplification factors (A) under various scenarios. STR corresponds to $N = 4$, and $\varepsilon_{a,1}/\varepsilon_{t,1} \approx 4$. Note that corresponding to $\theta_0 = 0$, the azimuthal parameter ϕ_0 is indeterminate and therefore dual parameter QFI's vanish. Hence the corresponding state is σ_{0,ϕ_0}.

4.4.3 QFI of a single qubit for quadrature observable

As explained in sec. 4.3.1 and in fig. 4.1(c), the first step of QST involves the direct quadrature detection of $\varrho_{\theta_0,\phi_0}$ to determine ϕ_0. Since the quadrature detection involves partitioning the original signal into real and imaginary parts (using a reference wave with 0 and $\pi/2$ phase-shifts [Lev08]), and as the data from each spectral line is analyzed independently, we may use the additivity property of QFI [Fri99] to obtain dual parameter quadrature QFI $\mathbb{F}_Q(\varrho_{\theta_0,\phi_0})$ (see Appendix 8.7)

$$\frac{1}{\mathbb{F}_Q(\varrho_{\theta_0,\phi_0})} = \inf\left\{\frac{4}{F_\theta(\varrho'_{\theta_0,\phi_0}, I_\alpha)}\right\} + \inf\left\{\frac{4}{F_\phi(\varrho_{\theta_0,\phi_0}, I_\alpha)}\right\}, \qquad (4.36)$$

where the infimum is taken over $\alpha \in \{x, y\}$. Table 4.2 lists the values of QFI $\mathbb{F}_Q(\varrho_{\theta_0,\phi_0})$ for various initial states. However, if the target qubit is known to be in the neighborhood of $\varrho_{\theta_0,\phi_0}$ (QST does not require this information), one can perform optimal (unbiased) measurements to obtain $\mathbb{F}(\varrho_{\theta_0,\phi_0})$ using eq. (4.25). The estimated values are also listed in Table 4.2.

4.4.4 QFI of an N-qubit STR for quadrature observable

The four observables used in eq. (4.12) together with the QST propagator U_T (see fig. 4.1(d)) are equivalent to the effective observables (in Heisenberg picture)

$$M_{q\alpha} = U_T^\dagger I_{q\alpha}^A U_T \qquad (4.37)$$

where $q \in \{0, 1\}$ and $\alpha \in \{x, y\}$ and $I_{q\alpha}^A$ are defined as in eq. (4.10). As described in Appendix 8.7, dual parameter quadrature QFI $\mathbb{F}_Q(\rho_{\theta_0,\phi_0})$ is

$$\frac{1}{\mathbb{F}_Q(\rho_{\theta_0,\phi_0})} = \inf\left\{\frac{4}{F_\theta(\rho_{\theta_0,\phi_0}, M_{q\alpha})}\right\} + \inf\left\{\frac{4}{F_\phi(\rho_{\theta_0,\phi_0}, M_{q\alpha})}\right\}, \qquad (4.38)$$

where infimum is over $q \in \{0, 1\}$ and $\alpha \in \{x, y\}$. The estimated values of QFI $\mathbb{F}_Q(\rho_{\theta_0,\phi_0})$ with QST observables and that of the QFI $\mathbb{F}(\rho_{\theta_0,\phi_0})$ with optimal measurements (i.e., as in eq. (4.35)) are also listed in Table 4.2. We find that the QFI $\mathbb{F}_Q(\rho_{\theta_0,\phi_0})$ corresponding to the quadrature measurement of the correlated target qubit is amplified by at least 6 times compared to the isolated (uncorrelated) qubit's QFI $\mathbb{F}_Q(\varrho_{\theta_0,\phi_0})$. Even the QFIs corresponding to the optimal measurements on the correlated target qubit are also amplified by a factor of at least 47 compared to that of the isolated qubit. Interestingly, it can be related to the polarization enhancement factor, which in the case of N-spin STR happens to be $(\varepsilon_{a,1}/\varepsilon_{t,1})\sqrt{N-1} = (\gamma_a/\gamma_t)\sqrt{N-1}$ [EBW04]. For acetonitrile this factor is about 6.93. Since QFI grows quadratically with the generalized Bloch radius and linearly with number of ancillary qubits, one can expect $6.93^2 \simeq 48$ to be the amplification factor as evident from Table 4.2. However $\mathbb{F}_Q(\rho_{\theta_0,\phi_0})$ is much less than the maximum QFI corresponding to SLD i.e., $\mathbb{F}(\rho_{\theta_0,\phi_0})$, this is because the former is obtained by QST-based observables with no prior information about the state of the target qubit, while the latter is obtained with optimized observables setup using the prior information that the target state is in the neighborhood of ρ_{θ_0,ϕ_0}.

4.5 Summary and conclusion

Quantum Fisher information (QFI) is a measure of sensitivity of an observable to small fluctuations in the value of a parameter corresponding to a given quantum state. It is an important tool to quantify the maximum achievable precision in measuring an unknown parameter with a given amount of resource. In this work, we worked with a star topology register (STR), which consists of a central target qubit surrounded by a set of identical ancillary qubits. While an STR does not allow any individual control on the ancillary qubits, it allows the target qubit to efficiently correlate with all the ancillary qubits, leading to several interesting applications. We showed that, if the target qubit is precorrelated with the ancillary qubits, it is possible to achieve a full QST of the target qubit by a single quadrature measurement of only ancillary qubits. We studied QFI of the target qubit that is precorrelated with ancillary qubits and compared it with QFI of the uncorrelated target qubit. In each case, we estimated QFI corresponding to (i) the observables used for QST (i.e., quadrature detection) with no prior information about the state of the target qubit and (ii) the optimal observables obtained given the state of the target qubit to be in the neighborhood of ρ_{θ_0,ϕ_0}. We showed that if the target qubit is initially precorrelated with ancillary qubits, we can achieve upto 8 times amplification in QFI compared to the uncorrelated case even with QST observables. We further showed that, with optimal observables, the QFI amplification is not only higher, but also scales linearly with the size of the STR, i.e., with the number of ancillary qubits and quadratically with the generalized Bloch radius $\varepsilon_{a,1}$ of ancillary qubits (for $\varepsilon_{a,1} \ll 1$). We believe that this protocol is a step towards realizing efficient quantum measurements applicable for a variety of quantum architectures including spin-based

69

architectures.

CHAPTER 5

Frequentist-approach inspired theory of quantum random phenomena: A theoretical exploration

"There is no law other than the law that there is no law."-J A Wheeler [bJDBDJ05].

5.1 Abstract

Different ensembles of the same density matrix are indistinguishable within the modern Kolmogorov probability measure theory of quantum random phenomena. We find that changing the framework from the Kolmogorov one to a frequentist-inspired theory of quantum random phenomena – à la von Mises – would lift the indistinguishability, and potentially cost us the no-signaling principle (i.e., lead to superluminal communication). We believe that this adds to the recent works on the search for a suitable representation of the state of a quantum system. While erstwhile arguments for potential modifications in the representation of the quantum state were restricted to possible variations in the formalism of the quantum theory, we indicate a possible fallout of altering the underlying theory of random processes.

5.2 Introduction

In this work we revisit the mathematical description of unknown state of a given quantum system and propose an approach which is alternative to the standard one. Born's statistical interpretation of the state vector in quantum mechanics (QM) and hence the density matrix description is based on Kolmogorov's modern axiomatic, probability-measure theoretic approach to random phenomena [Gut05, ST05, Ros10, Bil95, Wil10]. We refer to this as Kolmogorov QM (KQM) [Per02, CTDL05, MV10, Sha08, Gri95]. It is important to note that the convergence shown by strong law of large numbers (LLN) (which tries to justify the *a priori* assumed probability measure) is not pointwise but in terms of the very notion of probability [ST05, Spa13]. The parallel and earlier approach by von Mises employs a limiting relative frequency definition of probability, which assumes existence of the limit [VM81, Cra53, Haj12], while it (the limit) does not exist in a strict mathematical sense [Ros10, ST05, Spa13]. Here we take an approach to quantum random phenomena which is inspired by the frequentist one, but different. We refer to it as frequentist-inspired QM (FQM). Conceptually, FQM is same as pathwise or model-free approach to stochastic processes in mathematical finance, wherein a probability measure is not assumed *a priori* [Son06, Kar95, AC17, Rig16, Hob11]. We then show that such a frequentist-inspired approach leads to violation of the no-signaling principle [PT04, KB13, PR94, Per02] (i.e., leads to superluminal communication), by distinguishing between two different ensemble preparation procedures, which are indistinguishable in KQM, while still remaining within the Hilbert space formalism of quantum mechanics.

The main differences between KQM and FQM are the following: 1. KQM assumes *a priori* a constant value (i.e., a real number between 0 and 1) for the probability of even a single random event [Gut05]. Whereas in FQM, *a priori* probability measure is

dropped completely and instead an *a posteriori* limit-supremum of relative frequency (LRF) is considered [SKBSS20]. 2. Consequently in KQM, an average state (i.e., mixed density matrix), corresponding to the unknown state of a given quantum system, is considered [CTDL05, NC10]. Whereas in FQM, all possible states (i.e., state vectors) corresponding to the unknown state of a given quantum system, are considered path by path [SKBSS20].

This work is organized as follows. In Sec. 5.3, we introduce the FQM and show that two ensembles described by the same density matrix can be distinguished via content-dependent relative fluctuations. In Sec. 5.4 we show how, for practical purposes, one can use KQM along with FQM in a consistent way. In Sec. 5.5, we discuss the possibility of signaling within FQM. In Sec. 5.6, we discuss about the likely connection between Boltzmann's H-theorem and FQM. In Sec. 5.7, we briefly discuss about perfect anti-correlation of singlet even within FQM, and the case of finite number of trials. And we conclude in Sec. 5.8.

5.3 A frequentist-inspired approach to quantum random phenomena

Consider a random variable X which is the outcome of projectively measuring $|0\rangle\langle 0|$ on $|+\rangle$ where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, and $|0\rangle$ ($|1\rangle$) is the eigenstate of the Pauli-z observable, σ_z, with eigenvalue $+1$ (-1). X has the sample space $\{+1, 0\}$. Assume that the measurement can be repeated indefinitely, under exactly the same conditions, on identical copies of $|+\rangle$, independently. KQM assumes, *a priori*, a constant value for the probability of a single random event $X = +1$, based on the subjective notion of "equally likely" events, which is $P(X = +1) = 1/2$ (Born's statistical interpretation of

$|+\rangle$ [Gri95]) [Ros10, ST05, Gut05, Bil95, Wil10]. However in FQM, we suppose that the objective LRF of the event $X = +1$, denoted as $F(X = +1)$ (this plays the role of $P(X = +1)$), is obtained *a posteriori* via experiment as follows. Let X_i be the outcome of the ith trial of X. Then the number of $+1$ outcomes in N independent trials of X is given by $N_{+1}(X, N) = \sum_{i=1}^{N} X_i$. An operationally motivated definition of LRF of the event $X = +1$ is

$$F(X = +1) = \limsup_{N \to \infty} \frac{N_{+1}(X, N)}{N}$$
$$\equiv \lim_{N \to \infty} \left(\sup_{M \geq N} \frac{N_{+1}(X, M)}{M} \right) := \frac{1}{2} + \kappa(X = +1) \tag{5.1}$$

[Soh06, Roy68, Rud76, Mun07, Apo85, Gup16], where $\kappa(X = +1)$ is a random variable which takes values in $[-\epsilon, \delta]$ ($\epsilon > 0$, $\delta > 0$), depending on the outcomes in a given experiment. Note that in Eq. (5.1), $1/2$ cannot be preferred over $1/2 + c, |c| > 0$, due to fundamental indeterminacy. Only relative fluctuation matters. (See Appendix 8.8 for details.) $\kappa(X = +1)$ represents an intrinsic or fundamental fluctuation in $F(X = +1)$. $\kappa(X = +1)$ is a consequence of Knightian type of 'true' uncertainty [Kni21, BHD16, Hob11, Rig16]. It is important to note that this fluctuation in $F(X = +1)$ is due to an intrinsic random nature of outcomes of the trials, and not due to varying conditions from one experiment to another, including imperfections in preparing a quantum state which are unavoidable in the real world.

We also note that in the real world, we can realize $1 \ll N < \infty$ only, and noise in the state preparation and other type of noises like thermal, electronic etc., are unavoidable. Consequently it will add up with true/intrinsic fluctuation of $\kappa_N(X = +1)$ where $\limsup_{N \to \infty} \kappa_N(X = +1) = \kappa(X = +1)$. And hence we have to device some experimental techniques to get rid of or subtract out these noises (like in NMR) and obtain the true fluctuation of $\kappa_N(X = +1)$. Also noise may make discrimination between the two

different ensemble preparation procedures A and B (discussed below) difficult. However as the effect of noise is common to both the procedures A and B, and as we are interested only in the relative fluctuation, some kind of subtraction among the two fluctuations corresponding to the procedures A and B, may cancel the effect of noise.

Similarly, we also define $F(X = 0) = 1/2 + \kappa(X = 0)$. Further, we define the limit-infimum of relative frequency of the event $X = +1$ as follows: $F'(X = +1) = 1/2 + \kappa'(X = +1)$. Note that as $F(X = +1)$ and $F(X = 0)$ are independent, they need not sum to unity, unlike in $F'(X = +1) + F(X = 0) = 1$. However for $N < \infty$, as there is no need of supremum and infimum, we have $F_N(X = +1) + F_N(X = 0) = 1$ where $\limsup_{N \to \infty} F_N(.) = F(.)$, and $\liminf_{N \to \infty} F_N(.) = F'(.)$. Note that $F(X = +1)$ is a random variable, whereas $P(X = +1)$ is a constant. It is important to note that $\lim_{N \to \infty} N_{+1}(X, N)/N$ cannot always converge pointwise (in event space) [Rud76] to $1/2$, unlike, say, $\lim_{N \to \infty} 1/N = 0$ and $\lim_{N \to \infty} N_{+1}(X, N)/N^2 \leq \lim_{N \to \infty} 1/N = 0$ [ST05], Appendix 8.9. This is because $N_{+1}(X, N)$ is a random variable. The fundamental fluctuation in LRF can be considered as a *resource* within the frequentist-inspired theory of quantum random phenomena, in particular, as we show now, for distinguishing between two different ensemble preparation procedures of the same density matrix. This cannot be obtained within KQM due to *a priori* assuming constant values for the corresponding probabilities.

5.3.1 Distinguishing between two different ensemble preparation procedures for the same density matrix

Consider the two following preparation procedures.

Procedure A: In a trial of X, if the outcome is $+1$ (0), then Alice prepares a qubit in the state $|0\rangle$ ($|1\rangle$). She repeats the preceding step $\mathcal{M}$ times independently. She gives

this bunch – call it $\mathcal{E}_A$ – of $\mathcal{M}$ qubits to Bob.

Procedure B: This is the same as procedure A, except that $|0\rangle$ ($|1\rangle$) is replaced by $|+\rangle$ ($|-\rangle$). Again, Alice hands over this bunch – call it $\mathcal{E}_B$ – of $\mathcal{M}$ qubits to Bob.

Bob is aware of the two preparation procedures but unaware of the outcomes of trials of X. Further, Bob is allowed to choose the number $\mathcal{M}$ as large as he decides, carry out any unitary operation on the states, and measure any observable. The question is whether Bob can distinguish between the procedures A and B. The answer, within standard KQM, is in the negative, as the density matrix corresponding to both the procedures is the same, viz., $(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|)^{\otimes \mathcal{M}}$. We now consider the solution within FQM.

Instead of representing the states of the bunches, $\mathcal{E}_A$ and $\mathcal{E}_B$, in terms of density matrices, one may choose to represent them path by path as

$$
\begin{aligned}
|\psi_j^A\rangle &= \bigotimes_{i=1}^{\mathcal{M}} |X_i \oplus 1\rangle, \\
|\psi_j^B\rangle &= \bigotimes_{i=1}^{\mathcal{M}} |Z_i\rangle,
\end{aligned}
\tag{5.2}
$$

where $\oplus$ is addition modulo 2, $Z_i = +(-)$ if $X_i = +1(0)$, and $j \in \{1, 2, ..., 2^{\mathcal{M}}\}$ [LZJ$^+$06]. Particles in a bunch are noninteracting. Also, as particles in a bunch are distinguishable, Bob can ignore symmetrizing or anti-symmetrizing the total wave function representing the state of $\mathcal{E}_{A/B}$ [Sha08, TH06].

The state $|\psi_j^{A(B)}\rangle$ has all the information which Bob has about the given $\mathcal{E}_{A(B)}$. It may be noted that $|\langle \psi_j^A | \psi_k^B \rangle| = \frac{1}{2^{\mathcal{M}/2}} \neq 1, \forall j, k$. See [Pop18] and Appendix 8.10 in this respect. It may also be interesting to consider Refs. [Per96, AUČ$^+$05, Pal12] and references therein, where "superactivation of nonlocality" is considered within KQM.

Bob applies

$$R_x(X^\Theta) = \exp(-iX^\Theta \sigma_x/2) \tag{5.3}$$

to each of the qubits, where X^Θ is a random variable which outputs θ_i with LRF $F(X^\Theta = \theta_i) = 1/2 + \kappa(X^\Theta = \theta_i), i = 1, 2$. Then he measures σ_z on the qubit state.

Suppose, unknown to Bob, the bunch that he obtained was created by procedure A. Now, $R_x(X^\Theta = \theta_n)|0\rangle = |\theta_n, -\pi/2\rangle$, and $R_x(X^\Theta = \theta_n)|1\rangle = -i|\pi - \theta_n, \pi/2\rangle$, for $n = 1, 2$, where $|\theta, \phi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ in the usual Bloch sphere representation. Let X^θ be the outcome of measuring σ_z on $|\theta, \phi\rangle$. Then,

$$F(X^\theta = +1) = \cos^2(\theta/2) + \kappa(X^\theta = +1), \tag{5.4}$$

which is the *modified Born's statistical interpretation of* $|\theta, \phi\rangle$. Note that here we have assumed that the fluctuation term i.e., $\kappa(.)$ will depend on content/state i.e, θ. See Appendix 8.11 for its justification. And $F(X^\theta = -1) = \sin^2(\theta/2) + \kappa(X^\theta = -1)$, $\theta \neq 0, \pi$. Define sample mean as

$$S(A, M) = \frac{1}{M}\sum_{i=1}^{M} X_i^\theta, \tag{5.5}$$

where $A = \{X, X^\Theta, X^{\theta_1}, X^{\theta_2}, X^{\pi-\theta_1}, X^{\pi-\theta_2}\}$, $X_i^\theta \in \{X_i^{\theta_1}, X_i^{\theta_2}, X_i^{\pi-\theta_1}, X_i^{\pi-\theta_2}\}$. Let $M = 1$. Then

$$F(S(A, M = 1) = +1) = \limsup_{N\to\infty} \frac{N_{+1}(S(A, M = 1), N)}{N}. \tag{5.6}$$

The LRF, as defined in Eq. (5.1) or Eq. (5.6), is the only experimental or operational way to characterize or gain information about a given random variable. Hence, any

function we define should be expressible in terms of LRFs. The sample mean, as defined in Eq. (5.5) is one such function, as it can be rewritten as $\limsup_{N\to\infty} S(A, N) = 2F(S(A, M = 1) = +1) - 1$. It is the average of Bob's final σ_z measurement outcomes. (See Appendix 8.12 for details.)

We first consider the situation where $\theta_2 = \theta_1$. In this case, $N_{+1}(S(A, M = 1), N) = N_{+1}(X_1^{\theta_1}, N_{+1}(X_1, N)) + N_{+1}(X_1^{\pi-\theta_1}, N_0(X_1, N))$, where $N_0(X_1, N) = N - N_{+1}(X_1, N)$. We have

$$
\begin{aligned}
&\limsup_{N\to\infty} \frac{N_{+1}(X_1^{\theta_1}, N_{+1}(X_1, N))}{N_{+1}(X_1, N)} \frac{N_{+1}(X_1, N)}{N} \\
\leq\ &\limsup_{N\to\infty} \frac{N_{+1}(X_1^{\theta_1}, N_{+1}(X_1, N))}{N_{+1}(X_1, N)} \limsup_{N\to\infty} \frac{N_{+1}(X_1, N)}{N} \\
=\ &(\cos^2 \frac{\theta_1}{2} + \kappa(X_1^{\theta_1} = +1, +1(X_1)))(\frac{1}{2} + \kappa(X_1 = +1)),
\end{aligned}
\tag{5.7}
$$

for $N_{+1}(X_1, N \to \infty) > 0$ [Soh06, KN00]. In Eq. (5.6), using $\limsup_{N\to\infty}(x_N + y_N) \leq \limsup_{N\to\infty} x_N + \limsup_{N\to\infty} y_N$ where $\{x_N\}, \{y_N\}$ are sequences of real numbers [Roy68], and then substituting ineq. (5.7) and a similar result for $\limsup_{N\to\infty} N_{+1}(X_1^{\pi-\theta_1}, N_0(X_1, N))/N$, we get

$$
\begin{aligned}
F(S(A, M = 1) = +1) \leq\ &\frac{1}{2} \\
&+ \kappa(X_1 = +1)\left(\cos^2(\theta_1/2) + \kappa(X_1^{\theta_1} = +1, +1(X_1))\right) \\
&+ \kappa(X_1 = 0)\left(\sin^2(\theta_1/2) + \kappa(X_1^{\pi-\theta_1} = +1, 0(X_1))\right) \\
&+ \frac{1}{2}\left(\kappa(X_1^{\theta_1} = +1, +1(X_1)) + \kappa(X_1^{\pi-\theta_1} = +1, 0(X_1))\right).
\end{aligned}
\tag{5.8}
$$

(See Appendix 8.13 for details.) And $F(S(A, M = 1) = -1)$ will have a similar expression.

We note here that if we modify the KQM initial density matrix into $\rho^A = (1/2 +$

$\kappa(X = +1))|0\rangle\langle 0| + (1/2 + \kappa(X = 0))|1\rangle\langle 1|$, then one can easily verify that $R_x(X^\Theta = \theta_1)\rho^A R_x(X^\Theta = \theta_1)^\dagger$ along with the usual KQM Born rule for the subsequent σ_z-measurement do not reproduce the required result consistent with ineq. (5.8).

Next suppose that the bunch of $\mathcal{M}$ states that Bob obtained from Alice was prepared by procedure B. As before, Bob is oblivious of this choice of Alice. We have $R_x(X^\Theta = \theta_n)|\pm\rangle = e^{\mp i\theta_n/2}|\pm\rangle$, $n = 1, 2$. Therefore,

$$S(\mathrm{B}, M) = \frac{1}{M}\sum_{i=1}^{M} X_i^{\pi/2}, \tag{5.9}$$

where B $= \{X^{\pi/2}\}$. Then

$$
\begin{aligned}
&F(S(\mathrm{B}, M = 1) = +1) \\
&= \limsup_{N\to\infty} \frac{N_{+1}(S(\mathrm{B}, M = 1), N)}{N} \\
&= \frac{1}{2} + \kappa(X_1 = +1) \\
&= \frac{1}{2} + \kappa(X_1^\Theta = \theta_1),
\end{aligned}
\tag{5.10}
$$

since $X^{\pi/2}, X$, and X^Θ differ only in the value assigned to their outcomes (assuming $\theta_1 \neq \theta_2$; if $\theta_1 = \theta_2$ then X^Θ is not a random variable at all). And $F(S(\mathrm{B}, M = 1) = -1) = 1/2 + \kappa(X_1 = 0)$.

For $\theta_1 = 0, \pi/2$, ineq. (5.8) reduces to $F(S(\mathrm{A}, M = 1) = +1) = 1/2 + \kappa(X_1 = +1)$, because $N_{+1}(X_1^{\theta_1=0}, N_{+1}(X_1, N)) = N_{+1}(X_1, N)$. (See Appendix 8.14 for details.) However, in general the fluctuation of $F(S(\mathrm{A}, M = 1) = +1)$ (ineq. (5.8)) relative to that of $F(S(\mathrm{B}, M = 1) = +1)$ (Eq. (5.10)) is different. This is because, fluctuation of $\kappa(Y = y, Z)$ depends on both random variables Y and Z. And the expressions (5.8) and (5.10) are different functions of $\kappa(...)$'s and it is impossible to reduce ineq. (5.8) into Eq. (5.10). (Also see Fig. 5.1.) This is a necessary and sufficient condition for the

discrimination. (See Appendix 8.16 for further justification.) Assuming that there are no further physical restrictions on the observability of the fluctuations, we have therefore shown that our frequentist-inspired approach distinguishes equal density matrices.

Further it is important to note that as relative fluctuation (which do not require quantitatively precise prediction) is sufficient for discriminating between the two preparation procedures, it is not really necessary to use KQM (which gives quantitatively precise prediction) even in the later stages of the calculations as done in Appendix 8.20. Hence the discrimination between the two preparation procedures is predicted completely within FQM.

5.4   Using KQM along with FQM in a consistent way

If we use only FQM (KQM) then we obtain quantitatively imprecise (precise) predictions. FQM's prediction is quantitatively imprecise due to the fundamental fluctuation associated with $\kappa(...)$'s. Hence, we should use KQM along with FQM, but in a consistent way, to make predictions which are quantitatively precise as well. In fact, FQM or the "pathwise" approach is already being used (without it being stressed) in quantum teleportation [BBC$^+$93, NC10], approximate quantum cloning [BcvH96], the Bennett-Brassard 1984 quantum cryptography protocol [BB84], [NC10], discriminating between linearly independent [Che98] and dependent [BHW09] state vectors. In [BBC$^+$93], [BcvH96], [BB84], and [Che98, BHW09], the authors consider the unknown states ($|\psi\rangle$) to be teleported, cloned, cryptographed, and discriminated, respectively, within a path by path approach, and without assuming *a priori* a probability measure for Y, where a single copy of $|\psi\rangle$ has been prepared according to the outcome of a trial of a random variable Y. However they assume *a priori* a probability measure for other random variables. We note here that in pathwise approach of mathematical finance
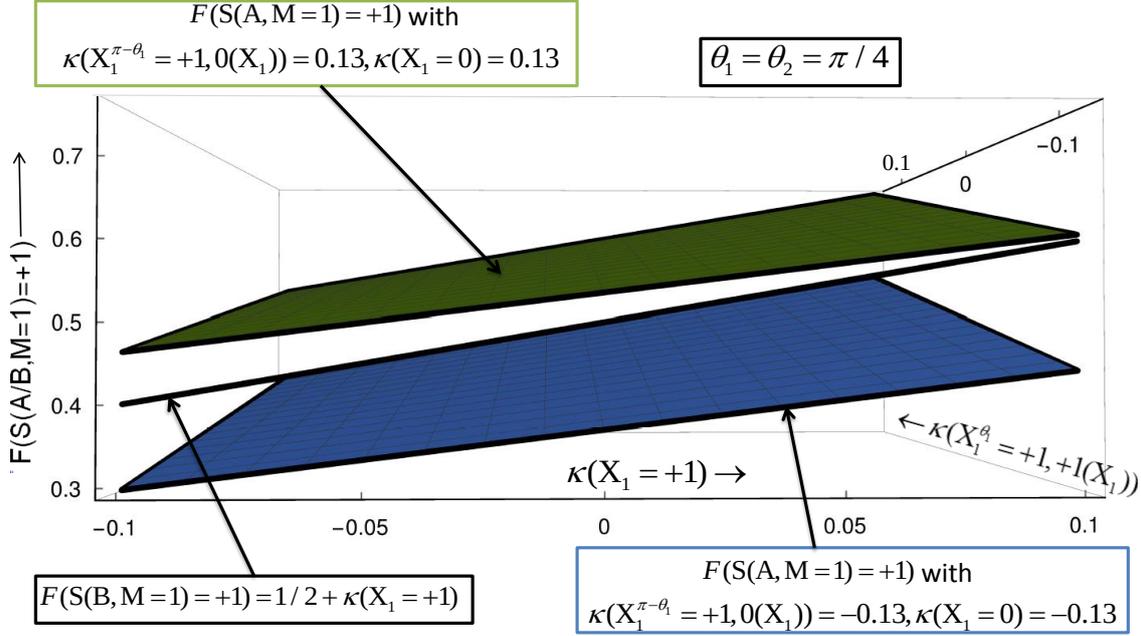
Fig. 5.1: Comparing the frequentist predictions for two preparation procedures A and B. We consider here the $\theta_1 = \theta_2$ case. We wish to compare $F(S(A, M = 1) = +1)$ with $F(S(B, M = 1) = +1)$. We set $\theta_1 = \theta_2 = \pi/4$. We have four independent random variables viz., $\kappa(X_1 = +1), \kappa(X_1 = 0)$, $\kappa(X_1^{\theta_1} = +1, +1(X_1))$, and $\kappa(X_1^{\pi-\theta_1} = +1, 0(X_1))$. We present a "front view" i.e., looking along the normal to the $(\kappa(X_1 = +1), F(S(A/B, M = 1) = +1))$-plane. Hence, plot for $F(S(B, M = 1) = +1)$ is the simple black straight line. However the bounds of $F(S(A, M = 1) = +1)$ are surfaces in the corresponding five-dimensional space. For given values of $\kappa(X_1^{\pi-\theta_1} = +1, 0(X_1))$ and $\kappa(X_1 = 0)$, the same are surfaces in the corresponding three-dimensional space. $\kappa(X_1^{\pi-\theta_1} = +1, 0(X_1))$ and $\kappa(X_1 = 0)$ can take both positive and negative values. Consider, first, an exemplary situation where $\kappa(X_1^{\pi-\theta_1} = +1, 0(X_1)) = -0.13$ and $\kappa(X_1 = 0) = -0.13$. This leads to the blue surface at the bottom for the bound of $F(S(A, M = 1) = +1)$ in ineq. (5.8). $F(S(A, M = 1) = +1|\kappa(X_1^{\pi-\theta_1} = +1, 0(X_1)) = -0.13, \kappa(X_1 = 0) = -0.13)$ can only be below the blue surface, and so must be different from $F(S(B, M = 1) = +1)$. The green surface, that is at the top for most of the considered region on the $(\kappa(X_1 = +1), \kappa(X_1^{\theta_1} = +1, +1(X_1)))$-plane, is the plot for the bound of $F(S(A, M = 1) = +1)$ in ineq. (5.8) with $\kappa(X_1^{\pi-\theta_1} = +1, 0(X_1)) = 0.13$ and $\kappa(X_1 = 0) = 0.13$. This time, $F(S(A, M = 1) = +1|\kappa(X_1^{\pi-\theta_1} = +1, 0(X_1)) = 0.13, \kappa(X_1 = 0) = 0.13)$ can only be below the green surface, and again there are regions where it is different from $F(S(B, M = 1) = +1)$. Hence in procedure A, there are points corresponding to LRF which are above, as well as below that corresponding to end points of the line segment $F(S(B, M = 1) = +1) = 1/2 + \kappa(X_1 = +1)$. The fluctuation of LRF, around $1/2$, will therefore be different in the two procedures. For ease of plotting, we have taken $|\kappa(\cdots)|$'s to be large. All quantities are dimensionless. Note that the surfaces in the above figure gives only the upper bounds. To know the corresponding lower bounds, we need to evaluate limit infimum. (See Appendix 8.15 for details.)

[Son06], probability measure is also brought in at a later stage of the analysis to study the interplay between all paths of a given stochastic process. We note that the two notions, *viz.*, assuming *a priori* a probability measure $p_{|\psi(y)\rangle}$ for Y and path by path consideration of $|\psi\rangle$'s, cannot exist simultaneously. If we assume *a priori* a probability measure then we are forced to consider the average mathematical state, $\int_{|\psi\rangle} dp_{|\psi\rangle} |\psi\rangle\langle\psi|$, instead of the actual physical states, $|\psi\rangle$ (see [BLSS09] in this regard).

5.5 Signaling

The distinguishing protocol discussed above can be used to provide instantaneous transfer of information between two separated locations. See [Pop14, PR94, Paw10, LHFL14] in this respect. Let Alice and Bob share $\mathcal{M}$ singlets $|S_0\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, and be space-like separated. If Alice measures $\sigma_z(\sigma_x)$ on her qubits, then on Bob's side $\mathcal{E}_{A(B)}$ is produced. As Bob can distinguish (at least in principle) between $\mathcal{E}_A$ and $\mathcal{E}_B$, he can know Alice's measurement choice superluminally. Note that we are not using nonlinear evolution to achieve signaling, like in [BHW09, LHFL14].

5.6 Connection to H-theorem

The Boltzmann entropy of a non-equilibrium physical system, increases with time, as per the H-theorem. However, the Gibbs-von Neumann entropy of the same system, is constant in time (consequence of Liouville's theorem). The two definitions of entropy agree in equilibrium systems [GLTZ19]. The Boltzmann entropy is defined within an approach where we consider the actual state of the given physical system (i.e., path by path approach [Son06, Kar95, AC17, Rig16, Hob11]) without assuming, *a priori*, a probability measure. Whereas, the Gibbs-von Neumann entropy is based on the density

matrix approach wherein we assume, *a priori*, a probability measure to obtain the average state of the system under consideration. The proof of the H-theorem depends on the definition of Boltzmann entropy, and crucially uses the hypothesis of "molecular chaos" or "past-hypothesis" or "typicality" [GLTZ19, Hua87, HPS$^+$06], along with the Hamiltonian dynamics, while the constancy of the Gibbs-von Neumann entropy uses the Hamiltonian dynamics only. It seems that the additional assumption akin to molecular chaos cannot be employed within the density matrix formalism of state description. See [GLTZ19, Kac56] in this regard. Assuming that to be true, this implies that averaging via a probability measure to obtain a density matrix, used in the Gibbs-von Neumann entropy, erases some information relevant to the dynamics of non-equilibrium systems.

5.7 Further aspects

Consider $S(\sigma_z^{\mathcal{A}}\sigma_z^{\mathcal{B}}, M) = (1/M)\sum_{i=1}^{M}\sigma_{zi}^{\mathcal{A}}\sigma_{zi}^{\mathcal{B}}$ where the random variable $\sigma_{zi}^{\mathcal{A}(\mathcal{B})}$ is the outcome of Alice (Bob) measuring σ_z on her (his) i^{th} qubit in the state $\alpha|01\rangle + \beta|10\rangle, |\alpha|^2 + |\beta|^2 = 1$. Then in FQM, one can easily show that $\lim_{N\to\infty} S(\sigma_z^{\mathcal{A}}\sigma_z^{\mathcal{B}}, N) = -1$. (See Appendix 8.17 for details.) Hence, even though one may feel that the randomness of $\kappa(\cdots)$ terms will get canceled by an extra randomness in the anti-correlation of the singlet and prevent signaling, such a thing does not happen, simply because such an extra randomness does not exist. Further, one may also feel that the randomness of $\kappa(\cdots)$ terms will get constrained by constraining the extra randomness in the anti-correlation of the singlet. This also does not happen for the same reason.

For $1 \ll N < \infty$, we obtain expressions which are same as the expressions (5.8), (5.10), but with $\kappa(\cdots)$'s replaced by the corresponding $\kappa_N(\cdots)$'s (which represent fluctuation corresponding to $1 \ll N < \infty$ such that $\limsup_{N\to\infty} \kappa_N(\cdots) = \kappa(\cdots)$), inequalities replaced by equalities, $\kappa_N(X = +1) + \kappa_N(X = 0) = 0$ and with similar constraint for

other $\kappa_N(\cdots)$ terms. This is because, when we take the limit $N \to \infty$, it turns out that the limit may not exist. Hence we have to consider limit supremum or limit infimum which always exists, and they give rise to inequalities. (See Appendix 8.18 for details.) Hence Bob can distinguish even when $1 \ll N < \infty$.

The case when $\theta_1 \neq \theta_2$ and the concept of using KQM in the later stages of calculations for practical purposes are considered in the Appendix 8.19 and Appendix 8.20 respectively.

Note that if we set $\kappa(\cdots)$'s to 0 in expressions (5.8), (5.10), we obtain the numerical values corresponding to the predictions of KQM. In this sense, KQM can be seen as a special case of FQM.

5.8   Conclusion

In summary, we found that a frequentist-inspired theory of quantum random phenomena leads to distinguishing between different ensembles of the same density matrix, which in turn leads to signaling (i.e., superluminal communication). This may be seen in the light of previous comments about the possible incompleteness of the density matrix representation, within modern Kolmogorov probability measure theory of quantum random phenomena, of a situation (state) of a physical system in Refs. [PSCWH00, LZJ+06, TH06, SK17, Pop18, Bel89, CM10]. To our knowledge, preceding discussions on possible modifications of the density matrix representation confined themselves to revisions of the description of the state within the Hilbert space formalism of quantum mechanics. We showed that remaining within the Hilbert space formalism but looking out for possible implications of variations of the underlying theory of random processes may cost us the no-signaling principle.

Violation of space-time Bell-CHSH inequality beyond Tsirelson bound and quantum cryptography

"The failure of Einstein separability violates, not the letter, but the spirit of special relativity..."-Popescu and Rohrlich [PR94]. (Quantum nonlocality has challenged Einstein's notion of separation in space and time.)

6.1 Abstract

Here we show that, if we insert context dependent local unitary evolutions into spatial (i.e., normal) Bell-CHSH test, then it is possible to violate space-time Bell-CHSH inequality maximally (i.e., up to 4). Correct context dependency can be achieved via post-selection. However this does not contradict Tsirelson quantum bound $(2\sqrt{2})$, because the latter has been derived without taking into consideration context dependent unitary evolutions and/or post-selection. As an important application, this leads to a more efficient (in terms of resource (singlets) and classical communication required) and more sensitive (to eavesdropping) quantum key distribution (QKD) protocol, compared to Ekert's and Wigner's QKD protocols [SK19].

6.2 Introduction

"Correlations cry out for explanation" - J S Bell [Bel89]. Assuming super-quantum correlations (PR box) and no-signaling (i.e., superluminal communication not possible), Popescu and Rohrlich have shown that one can violate Bell's inequality [Bel64, CHSH69, NC10] upto its algebraic bound (i.e., 4) [PR94]. Cabello has also proposed a post-selection (on GHZ state) based Bell test to achieve the algebraic bound [Cab02]. Here we propose yet another scheme to achieve the same. In the spatial (i.e., normal) Bell-CHSH test, there is no unitary evolution. Alice and Bob randomly choose their observables and directly measure them locally on their respective entangled qubit states. As entangled particles are correlated over space in spite of measurement events being space-like separated (nonlocal correlation), correlation between Alice's and Bob's measurement outcomes can go up to $2\sqrt{2}$, there by violating local realistic bound 2 [NC10].

Here we show that it is possible to boost the correlation over space (which led to $2\sqrt{2}$) further, via context dependent local unitary evolutions. But this requires for Bob to know what Alice has measured (i.e., Alice's choice of her observable only, but not her outcome of measuring the corresponding observable), which is not possible unless Alice can signal Bob (because they are space-like separated) [SKBSS20]. We showed in chapter 5 that, in frequentist-inspired quantum mechanics, signaling is possible. However here we also provide a scheme wherein need for signaling can be bypassed as follows. Bob applies local unitary operations randomly, and then measures his observables. After all the measurements are performed, Alice and Bob post-select correct context dependent local unitarily evolved states via classical communication. By this procedure, Alice and Bob can achieve maximum possible correlation (i.e., 4) between their observables. However, this does not contradict Tsirelson quantum bound $(2\sqrt{2})$, as the latter has been

derived without taking into consideration context dependent local unitary evolutions and/or post-selection [Cir80, NC10].

As an important application, our new scheme leads to a more efficient and more sensitive (to eavesdropping) quantum key distribution (QKD) protocol. QKD or quantum cryptography is a provably secure protocol using which private key bits can be generated between two parties over a public channel [NC10]. Security of QKD protocols is based on the fact that, eavesdropper cannot steal the information without disturbing the quantum state [HPS17, Paw10, BBB$^+$06, BF02, LM05, May01, SP00, LC99, IH05, WTY06, Kra16, SR08, Ral00, YLC$^+$10, BKH$^+$16, AAP11]. Suppose Alice wants to send Bob a secret message 'Hi'. They some how have shared a secret key 'qw' (e.g., they met personally in the past and shared (but this is not always feasible) or via QKD). Alice mixes her secret message with the secret key (encryption) and obtains 'Hi+qw=rd'. Alice sends 'rd' to Bob over public channel. Then Bob decrypts the message to retrieve original secret message: 'rd-qw=Hi'.

There are many types of QKD protocols, chief among them are as follows. BB84 [BB84] and it's variants (not based on Bell's theorem for security) [NC10, JSW$^+$00, Ben92, Kak00]. Ekert's QKD protocol [Eke91] and its variants [BBM92, GRTZ02], and device independent QKD protocols which use entanglement and/or violation of Bell's inequality for their security [BKH$^+$16, MPA11, BCK12, VV14, YCY$^+$16, HPS17]. QKD via orthogonal states [GV95, ABD$^+$10]. (Semi)Counterfactual QKD protocols ([SSS13]) [Noh09, SW10, HPS17]. Continuous variable QKD protocols [Ral99, Hil00, GG02, Rei00, HPS17, DUF16]. Doing QKD considering noise in the channel [STP$^+$16, TPB17].

Our space-time (ST) QKD protocol exploits violation of Bell's inequality for security. In our ST QKD protocol half of the total resource (singlets) corresponds to correct context dependent unitarily evolved states. A small randomly chosen subset of this is utilized to test for eavesdropping, and the remaining large portion is utilized for secret

key bits generation. We are going to show that our ST QKD protocol is more efficient (in terms of resource (singlets), and classical communication (CC) required to generate a given amount of secret key bits), and more sensitive (to eavesdropping) than Ekert's and Wigner's QKD protocols. QKD has become important, because the security of public key distribution protocols, like RSA, is under threat with the advent of quantum computers, which can find the prime factors of large numbers in polynomial time (Shor's algorithm) [NC10, PMA$^+$19].

In Sec. 6.3 we describe ST Bell-CHSH test using post-selection. In Sec. 6.4 we propose our ST QKD protocol and compare it with other existing QKD protocols, and finally we summarize and conclude in Sec. 6.6.

6.3   Space-time Bell-CHSH test

Let Alice and Bob share N number of singlets:

$$|S_0\rangle = (|01\rangle - |10\rangle)/\sqrt{2} = -(|+-\rangle - |-+\rangle)/\sqrt{2},$$

where $|0\rangle, |1\rangle$ are eigenkets of Pauli-z matrix σ_z with eigenvalues $+1, -1$ respectively, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice's and Bob's clocks are synchronized and their measurement events are space-like separated. At time $t = t_j^A$, Alice measures locally the observable

$$A = \sigma_z \otimes I \quad \text{or} \quad C = \sigma_x \otimes I$$

on her j^{th} qubit state (i.e., she measures σ_z or σ_x on her qubit state), according to the outcome of an unbiased coin toss, $j = 1, 2, ..., N$, I is the 2×2 identity matrix.

Immediately after Alice's measurement, Bob applies unitary operator

$$U_{\pm y} = \exp\left(\mp i\frac{\pi}{4}\frac{\sigma_y}{2}\right) \tag{6.1}$$

to his j^{th} qubit state where U_k is chosen randomly from the set $\{U_{+y}, U_{-y}\}$ with probability $\{1/2, 1/2\}$ respectively, $j = 1, 2, ..., N$. Then at time $t = t_j^B (> t_j^A)$, Bob measures locally the observable

$$B = -I \otimes (\sigma_z + \sigma_x)/\sqrt{2} \quad \text{or} \quad D = I \otimes (\sigma_z - \sigma_x)/\sqrt{2}$$

on his j^{th} qubit state, according to the outcome of an unbiased coin toss, $j = 1, 2, ..., N$ [NC10].

Bob knows each of the N number of t_j^As. As collapse is instantaneous (which is evident from violation of spatial Bell-CHSH inequality [GBNP01, HBD+15]), Bob can carry out his operations immediately after Alice measures. We have the following eigenvalue equations:

$$\sigma_z|0\rangle = |0\rangle, \sigma_z|1\rangle = -|1\rangle, \sigma_x|\pm\rangle = \pm|\pm\rangle,$$
$$\frac{-(\sigma_z + \sigma_x)}{\sqrt{2}}|\pm\rangle_B = \pm|\pm\rangle_B, \frac{\sigma_z - \sigma_x}{\sqrt{2}}|\pm\rangle_D = \pm|\pm\rangle_D \tag{6.2}$$

where

$$|+\rangle_B = \cos(\theta_1/2)|0\rangle + e^{i\pi}\sin(\theta_1/2)|1\rangle,$$
$$|-\rangle_B = \cos(\theta_2/2)|0\rangle + \sin(\theta_2/2)|1\rangle,$$
$$|+\rangle_D = \cos(\theta_2/2)|0\rangle + e^{i\pi}\sin(\theta_2/2)|1\rangle,$$
$$|-\rangle_D = \cos(\theta_1/2)|0\rangle + \sin(\theta_1/2)|1\rangle, \tag{6.3}$$

89

$\theta_1 = \pi - \pi/4, \theta_2 = \pi/4$. Quantum mechanically the values of measurement outcomes a, c, b, d ($= \pm 1$, the eigenvalues) of observables A, C, B, D respectively, are not preassigned before the measurement process. b, d depends on Alice's choice of observable, even though their measurement events are space-like separated. Measurement creates reality [Per91, KS67, Mer90, EPR35, GHH$^+$14, Cav18].

When Alice measures A locally, if her qubit collapses to $|0\rangle$ or $|1\rangle$, then Bob's qubit always collapses instantaneously to $|1\rangle$ or $|0\rangle$ respectively (spatial correlation due to entanglement). Similarly when Alice measures C locally, if her qubit collapses to $|\pm\rangle$, then Bob's qubit collapses to $|\mp\rangle$.

6.3.1   Post-selected perfectly (anti)correlated sub-ensembles

After N measurements, they select out (via classical communication) the following four (out of eight) subensembles ($\mathcal{E}_i, i = 1, 2, 3, 4$) which corresponds to applying correct context dependent local unitary evolutions ($U_{\pm y}$):

($\mathcal{E}_1$) Alice had measured A, then Bob had evolved his qubit state under the unitary U_{+y} (i.e., counter clock wise rotation about y-axis by 45° on the Bloch sphere) to get $U_{+y}|1\rangle = |+\rangle_B$ or $U_{+y}|0\rangle = |-\rangle_B$, and then Bob had measured B. Then the product of measurement outcomes becomes $ab = +1 \times +1 = 1$ or $ab = -1 \times -1 = 1$. Hence knowing b, Bob can know a i.e., $a = b$ (perfectly correlated). Hence $\langle A(t^A)B_1(t^B)\rangle = 1 = ab_1$ where B_i, D_i represents association of B, D respectively with unitary evolution $U_{\mu_i}, i = 1, 2, \mu_1 = +y, \mu_2 = -y$, and b_i, d_i are measurement outcomes corresponding to B_i, D_i respectively, $i = 1, 2$. More rigorously, joint probability of Alice getting outcome a in a measurement of A and Bob, after applying U_{+y}, getting outcome b in a measurement of

B is given by

$$p(a, b|U_{+y}) = \text{Tr}(\mathcal{B}_b^{(2)} U_{+y}^{(2)} \mathcal{A}_a^{(1)} \rho_0 \mathcal{A}_a^{(1)} (U_{+y}^{(2)})^\dagger) \tag{6.4}$$

[Lö06, BE14], where $a, b = +1, -1$, $\rho_0 = |S_0\rangle\langle S_0|$,

$$\mathcal{A}_{+1}^{(1)} = |0\rangle\langle 0| \otimes I, \mathcal{A}_{-1}^{(1)} = |1\rangle\langle 1| \otimes I$$

$$\mathcal{B}_{\pm 1}^{(2)} = I \otimes |\pm\rangle_B\langle\pm|_B, U_{\pm y}^{(2)} = I \otimes U_{\pm y}.$$

$$\Rightarrow \langle A(t^A)B_1(t^B)\rangle = \sum_{a,b} p(a, b|U_{+y}) \, ab = 1 = ab_1, \tag{6.5}$$

where

$$p(a = +1, b = +1|U_{+y}) = p(a = -1, b = -1|U_{+y}) = 1/2,$$

$$p(a = +1, b = -1|U_{+y}) = p(a = -1, b = +1|U_{+y}) = 0.$$

($\mathcal{E}_2$) Alice had measured A, then Bob had evolved his qubit state under the unitary U_{-y} (i.e., clock wise rotation about y-axis by 45° on the Bloch sphere) to get $U_{-y}|1\rangle = |-\rangle_D$ or $U_{-y}|0\rangle = |+\rangle_D$, and then he had measured D. Then the product of measurement outcomes becomes $ad = +1 \times -1 = -1$ or $ad = -1 \times +1 = -1$. $\Rightarrow a = -d$ (perfectly anticorrelated). Hence $\langle A(t^A)D_2(t^B)\rangle = -1 = ad_2$. More rigorously, joint probability of Alice getting outcome a in a measurement of A and Bob, after applying U_{-y}, getting outcome d in a measurement of D is given by

$$p(a, d|U_{-y}) = \text{Tr}(\mathcal{D}_d^{(2)} U_{-y}^{(2)} \mathcal{A}_a^{(1)} \rho_0 \mathcal{A}_a^{(1)} (U_{-y}^{(2)})^\dagger) \tag{6.6}$$

where $a, d = +1, -1$, and $\mathcal{D}^{(2)}_{\pm 1} = I \otimes |\pm\rangle_D \langle \pm|_D$.

$$\Rightarrow \langle A(t^A) D_2(t^B) \rangle = \sum_{a,d} p(a, d|U_{-y}) \, ad = -1 = ad_2, \tag{6.7}$$

where

$$p(a = +1, d = +1|U_{-y}) = p(a = -1, d = -1|U_{-y}) = 0$$

$$p(a = +1, d = -1|U_{-y}) = p(a = -1, d = +1|U_{-y}) = 1/2.$$

$(\mathcal{E}_3)$ Alice had measured C, then Bob had evolved his qubit state under the unitary U_{-y} to get $U_{-y}|-\rangle = |+\rangle_B$ or $U_{-y}|+\rangle = |-\rangle_B$, and then he had measured B. Then the product of measurement outcomes becomes $cb = +1 \times +1 = 1$ or $cb = -1 \times -1 = 1$. $\Rightarrow c = b$ (perfectly correlated). Hence $\langle C(t^A) B_2(t^B) \rangle = 1 = cb_2$. More rigorously, joint probability of Alice getting outcome c in a measurement of C and Bob, after applying U_{-y}, getting outcome b in a measurement of B is given by

$$p(c, b|U_{-y}) = \text{Tr}(\mathcal{B}^{(2)}_b U^{(2)}_{-y} \mathcal{C}^{(1)}_c \rho_0 \mathcal{C}^{(1)}_c (U^{(2)}_{-y})^\dagger) \tag{6.8}$$

where $c, b = +1, -1$, and $\mathcal{C}^{(1)}_{\pm 1} = |\pm\rangle\langle\pm| \otimes I$.

$$\Rightarrow \langle C(t^A) B_2(t^B) \rangle = \sum_{c,b} p(c, b|U_{-y}) cb = 1 = cb_2, \tag{6.9}$$

where

$$p(c = +1, b = +1|U_{-y}) = p(c = -1, b = -1|U_{-y}) = 1/2,$$

$$p(c = +1, b = -1|U_{-y}) = p(c = -1, b = +1|U_{-y}) = 0.$$

92

($\mathcal{E}_4$) Alice had measured C, then Bob had evolved his qubit state under the unitary U_{+y} to get $U_{+y}|-\rangle = |+\rangle_D$ or $U_{+y}|+\rangle = |-\rangle_D$, and then he had measured D. Then the product of measurement outcomes becomes $cd = +1 \times +1 = 1$ or $cd = -1 \times -1 = 1$. $\Rightarrow c = d$ (perfectly correlated). Hence $\langle C(t^A)D_1(t^B)\rangle = 1 = cd_1$. More rigorously, joint probability of Alice getting outcome c in a measurement of C and Bob, after applying U_{+y}, getting outcome d in a measurement of D is given by

$$p(c, d|U_{+y}) = \text{Tr}(\mathcal{D}_d^{(2)} U_{+y}^{(2)} \mathcal{C}_c^{(1)} \rho_0 \mathcal{C}_c^{(1)} (U_{+y}^{(2)})^\dagger), \tag{6.10}$$

where $c, d = +1, -1$.

$$\Rightarrow \langle C(t^A)D_1(t^B)\rangle = \sum_{c,d} p(c, d|U_{+y}) cd = 1 = cd_1, \tag{6.11}$$

where

$$p(c = +1, d = +1|U_{+y}) = p(c = -1, d = -1|U_{+y}) = 1/2$$
$$p(c = +1, d = -1|U_{+y}) = p(c = -1, d = +1|U_{+y}) = 0.$$

Now substituting the above expectation values into the ST Bell-CHSH term we obtain

$$\langle I_Q \rangle = \langle A(t^A)B_1(t^B)\rangle + \langle C(t^A)B_2(t^B)\rangle$$
$$+\langle C(t^A)D_1(t^B)\rangle - \langle A(t^A)D_2(t^B)\rangle = 4$$
$$= ab_1 + cb_2 + cd_1 - ad_2 = I_Q, \tag{6.12}$$

which is the maximum possible violation of classical (local) upper bound 2. I_Q takes only one value i.e., 4. Hence $\langle I_Q \rangle = I_Q = 4$ (i.e., there is no variance/error in experimentally evaluating the expectation value). $\langle I_Q \rangle = 4$ does not contradict Tsirelson bound $(2\sqrt{2})$

[Cir80, NC10], because there are local unitary evolutions involved, and Alice and Bob are post-selecting the correct context dependent local unitarily evolved subensembles. Both of these are not considered in deriving Tsirelson bound.

There are two context dependencies here: (1) Whether Bob measures B in the context of A or in the context of C (A and C do not commute). This context dependency manifests as nonlocal correlation over space, as measurement events are space-like separated [Per91, KS67, GHH$^+$14, Cav18]. Similar context dependency for D. This results in $2 < \langle I_Q \rangle \le 2\sqrt{2}$. (2) The context dependent local unitary operations that Bob applies to his qubit states, as described above. This boosts the nonlocal correlation over space that is already present, to the maximum extent possible. If there was no nonlocal correlation over space (like in classical scenario), then unitary evolution cannot boost the correlation any further. Hence even though no entanglement during unitary evolution, we are able to boost the correlation as there was entanglement (correlation) prior to unitary evolution. State of Bob's qubit gets maximally (anti)correlated (with respect to measurement outcomes) with that of Alice's, as Bob applies $U_{\pm y}$. This results in $2\sqrt{2} < \langle I_Q \rangle \le 4$. In other words, during unitary evolution, Bob's qubit evolves into such a state that measurement outcomes of Alice and Bob gets perfectly (anti)correlated.

As the singlet state $|S_0\rangle$ is Bell nonlocal, it is also EPR steerable. This is because Bell nonlocality implies EPR steerability [QVC$^+$15, TNA16, WJD07]. Further in our protocol, Alice and Bob use classical communication for post-selecting the correct context dependent local unitarily evolved subensembles, and Bob uses local unitary operations only. Hence the operations used by Alice and Bob (i.e., LOCC) are the natural free operations of the resource theory of entanglement [GA15].

Further note that, if we calculate the expectation values without post selecting the strongly correlated sub-ensembles, then we obtain $\langle I_Q \rangle = 2$. This is because the strong correlation built up due to correct context dependent $U_{\pm y}$, is destroyed by the wrong

context dependent $U_{\pm y}$. If we do not apply $U_{\pm y}$ at all, then we get $\langle I_Q \rangle = 2\sqrt{2}$ [NC10].

6.4 A more efficient and more sensitive ST QKD protocol

In the above ST Bell-CHSH test, Alice and Bob use a small portion of subensembles $\mathcal{E}_1$ to $\mathcal{E}_4$, to test for eavesdropping/noise in the quantum channel. Remaining large portion of the subensembles $\mathcal{E}_1$ to $\mathcal{E}_4$ is used for secret key bits generation. Note that to separate the subensembles $\mathcal{E}_1$ to $\mathcal{E}_4$ from $\mathcal{E}_5$ to $\mathcal{E}_8$ (which corresponds to states evolved under wrong context dependent $U_{\pm y}$), they need to publicly announce only their sequence of random choice of observables, and Bob's sequence of random choice of U_{+y}, U_{-y}, but not their measurement outcomes.

6.4.1 Test for eavesdropping

Alice and Bob test for eavesdropping as follows: They publicly announce a few set of measurement outcomes chosen from the subensembles $\mathcal{E}_1$ to $\mathcal{E}_4$ (they need not choose it randomly because see Sec. 6.4.3), and look for their perfect correlation ($a = b_1, c = b_2, c = d_1$) and perfect anticorrelation ($a = -d_2$). Perfect correlation/anticorrelation in each set of measurement outcomes is possible if and only if particles were maximally entangled in each set (which implies no eavesdropping). They can also look for $\langle I_Q \rangle = 4$, as it does not require an ensemble ($\because \langle I_Q \rangle = I_Q$ (Eq. (6.12)), and hence a minimum of four sets of measurement outcomes are sufficient to calculate $\langle I_Q \rangle$), unlike in Ekert and Wigner protocols which requires an ensemble of large number of set of measurement outcomes (see Sec. 6.4.4 for justification; also see Table 6.1). If they obtain perfect correlation/anticorrelation in more than, say, n (threshold value considering noise in

the channel) sets of measurement outcomes, then they can safely conclude that there was no eavesdropping, and hence they can generate secret key bits. Else they have to discard the keys and start afresh.

6.4.2 Secret key bits generation

If there was no eavesdropping, then they can generate secret key bits using the remaining large portion of subensembles $\mathcal{E}_1$ to $\mathcal{E}_4$ (whose outcomes are not publicly announced) as follows: Bob knows whether B has been measured in the context of A or C. Similarly D. Further $a = b_1, c = b_2, c = d_1$ (perfectly correlated). Hence both Alice's and Bob's measurement outcomes will be either $+1$ or -1. Hence they directly obtain the keys. Whereas $a = -d_2$ (perfectly anticorrelated). Hence if Alice's outcome is ± 1, then Bob's outcome will be ∓ 1. Hence one of them has to invert to obtain the keys.

6.4.3 Amount of classical communication required

Ekert QKD protocol: Alice and Bob use three observables each [JSW$^+$00]. They assign $0, 1, 00$ to their observables. Hence each require approximately $N/3 + N/3 + 2N/3 = 4N/3$ bits of classical communication (CC) to publicly announce their sequence of random choice of observables. To test for eavesdropping, one of them has to announce their measurement outcomes of 4 subensembles out of 9, which requires $4N/9$ bits of classical communication. Hence total CC required is $28N/9 = 14M$ bits ($\because N = M/K$ where K and M are defined in Table 6.1).

Wigner QKD protocol: Alice and Bob use two observables each [JSW$^+$00]. They assign $0, 1$ to their observables. Hence each require approximately $N/2 + N/2 = N$ bits of CC to publicly announce their sequence of random choice of observables. To test for eavesdropping, one of them has to announce their measurement outcomes of 3 subensembles

out of 4, which requires $3N/4$ bits of classical communication. Hence total CC required is $11N/4 = 11M$ bits.

ST QKD protocol: Alice and Bob use two observables each. Hence each require approximately $N/2 + N/2 = N$ bits of classical communication (CC) to publicly announce their sequence of random choice of observables. Further Bob require $N/2 + N/2 = N$ bits of CC to publicly announce his sequence of random choice of U_{+y}, U_{-y}. They choose, say, first or last or middle ϵN out of $N/2$ measurements which correspond to correct context dependent unitarily evolved states, to test for eavesdropping. In fact they can choose any consecutive ϵN out of $N/2$ measurements which correspond to correct context dependent unitarily evolved states, to test for eavesdropping. Note that there is no need to choose it randomly, because the $N/2$ measurements which correspond to correct context dependent unitarily evolved states were themselves randomly distributed. That is, the elements of subensembles $\mathcal{E}_1$ to $\mathcal{E}_4$ were themselves randomly distributed among N singlets shared between Alice and Bob. Other four subensembles were discarded. Hence Eve cannot know *a priori* which singlet is going to be an element of $\mathcal{E}_1$ to $\mathcal{E}_4$. Hence she has to attack on each of the N singlets. Hence there is no need to further randomly choose a small subset, from $\mathcal{E}_1$ to $\mathcal{E}_4$, to test for eavesdropping. Hence one of them require ϵN bits of CC to announce the corresponding measurement outcomes, to test for eavesdropping. Hence total CC required is $N(3 + \epsilon) = 2M(3 + \epsilon)/(1 - 2\epsilon)$ bits.

BB84′ QKD protocol (a variant of BB84 with entangled photons (see Ref. [JSW$^+$00])): Alice and Bob use two observables each [JSW$^+$00]. Hence each require approximately $N/2 + N/2 = N$ bits of classical communication (CC) to publicly announce their sequence of random choice of observables. To test for eavesdropping they require ϵN bits of CC as in ST QKD protocol. Hence total CC required is $N(2 + \epsilon) = 2M(2 + \epsilon)/(1 - 2\epsilon)$ bits. These are tabulated in Table 6.1.

6.4.4 Sensitivity to eavesdropping

Whatever the eavesdropping strategy, it is known that monogamy of entanglement provides/ensures security of QKD protocol even if the eavesdropper has access to signaling resources [Paw10]. Hence here we define a sensitivity criterion which is independent of the eavesdropping strategy. Consider Ekert QKD protocol [Eke91]. He uses Bell CHSH expression with a global negative sign. Hence consider $\langle AB \rangle_{\rho_0}$ where symbols are as defined earlier. Strong LLN asserts that [Ros10]

$$P\left(\lim_{n \to \infty} F_n^{\text{expt}}(\langle AB \rangle_{\rho_0}) = \langle AB \rangle_{\rho_0} \right) = 1. \tag{6.13}$$

where $F_n^{\text{expt}}(\langle AB \rangle_{\rho_0}) = \sum_{i=1}^{n} \frac{A_i B_i}{n}$ where $A_i(B_i)$ is the outcome of i-th local measurement of $A(B)$ on ρ_0. Variance $\text{Var}(F_n^{\text{expt}}(\langle AB \rangle_{\rho_0})) = \text{Var}(AB)/n$ where $\text{Var}(AB) = \langle (AB)^2 \rangle_{\rho_0} - \langle AB \rangle_{\rho_0}^2$. Define intrinsic error due to randomness in measurement outcomes as,

$$\Delta_n^{\text{intrinsic}} = |F_n^{\text{expt}}(\langle AB \rangle_{\rho_0}) - \langle AB \rangle_{\rho_0}| = c/\sqrt{n} \tag{6.14}$$

where c is a constant which depends on $\text{Var}(AB)$ and the confidence level required. Define extrinsic error due to eavesdropping and noise in the channel

$$\Delta_n^{\text{extrinsic}} = \Delta_n^{\text{total}} - \Delta_n^{\text{intrinsic}} \propto \text{amount of eavesdropping and noise in the channel.}$$

$$\tag{6.15}$$

Define sensitivity at a given m

$$\mathcal{S}_m = (4\Delta_n^{\text{extrinsic}} - 4\Delta_n^{\text{intrinsic}})/(4\Delta_n^{\text{extrinsic}}) \tag{6.16}$$

where $m = 4n$, and we have assumed that there will always be nonzero noise in the channel and hence $\Delta_n^{\text{extrinsic}} > 0$. And factor 4 is because there are four terms in the Bell expression and errors being random, they add up. Hence $\mathcal{S}_m \leq 1$. Hence in Ekert QKD protocol, larger the m, better is the sensitivity of the protocol to eavesdropping. And smaller the m, less sensitive is the protocol to eavesdropping. A similar result holds for Wigner QKD protocol as well. However in ST-QKD protocol, $\Delta_n^{\text{intrinsic}}$ is zero for arbitrary n. This is because every pair in $\mathcal{E}_1$ to $\mathcal{E}_4$ is either perfectly correlated or anti-correlated. Hence $A(t^A)B_1(t^B) = 1, C(t^A)B_2(t^B) = 1, C(t^A)D_1(t^B) = 1, A(t^A)D_2(t^B) = -1$ always. Hence for any given m, $\mathcal{S}_m = 1$. This is also a consequence of achieving the algebraic bound 4. Hence for any given value of n, ST-QKD protocol is more sensitive to eavesdropping than Ekert and Wigner QKD protocols. Strictly speaking, this holds even in the limit $n \to \infty$ because intrinsic fluctuation never dies by virtue of $\kappa(.)$ terms (see chapter 5 for details).

Sensitivity and key rate

Let us fix n. One can verify that

$$\text{Var}(AB) = 1 - \text{Cov}(A, B)^2 \tag{6.17}$$

where $\text{Cov}(A, B) = \langle AB \rangle_{\rho_0} - \langle A \rangle_{I/2} \langle B \rangle_{I/2} = \langle AB \rangle_{\rho_0}$ [Ros10]. Hence c in Eq. (6.14) will decrease as the $\text{Cov}(A, B)$ (and hence the amount of violation of Bell or Bell type inequality) increases. Which in turn implies enhancement in S_m. Hence for a given m, larger the violation of Bell inequality, more is the S_m.

Now to achieve a given value of S_m, we have to increase n and/or amount of violation of Bell inequality. Hence it is possible to reduce n by increasing the amount of Bell inequality violation. This in turn implies less wastage (T in Table 6.1) and hence an

increase in key rate.

A comparison of our ST QKD protocol with other QKD protocols is given in Table 6.1. It is evident from the table that ST QKD protocol is more efficient (in terms of resource N and CC required to generate a given amount of secret key bits), and more sensitive (to eavesdropping) than Ekert's and Wigner's QKD protocols. This is achieved at the cost of introducing a simple local unitary evolution. ST is as efficient as BB84$'$ in all aspects except in the CC required (but BB84$'$ belongs to a different group i.e., it is not based on Bell's theorem).

In Ekert's and Wigner's QKD protocols, the constraint $T \times N \ggg 1$ (T, N defined in Table 6.1) must be satisfied to kill the error/variance in calculating expectation values corresponding to Bell's inequality (hence large ensemble measurement is necessary). But it is not required in ST QKD protocol as the products $ab_1 = +1, cb_2 = +1, cd_1 = +1, ad_2 = -1$ (Eq. (6.12)) always (i.e., no variance in these products), unlike in Ekert's and Wigner's QKD protocols. See Sec. 6.4.4 for details. Hence, when M is small (i.e., only a small amount of secret key bits are required), only ST and BB84$'$ are economical.

Further we note that, if Bob can store his qubit states in quantum memory till Alice publicly announces her sequence of random choice of measurement observables, then all entries in discard (D) column (Table 6.1) can be made zero. This is because, discarding of singlets corresponding to discard column is solely because Bob do not know *a priori* Alice's choice of her measurement observable. Hence if Bob stores his qubit states in quantum memory until Alice announces her choice of measurement observable on a given singlet, then Bob can subsequently apply the correct $U_{\pm y}$ and choose appropriate/correct observable to be measured. By this, discarding of singlets can be completely eliminated. By this eavesdropper will not gain any advantage. Consequently, more key bits can be generated in Ekert, ST, and BB84$'$. But storing quantum states against decoherence is a great challenge.

100

Table 6.1: Ek, Wi, ST, and B′ stands for Ekert, Wigner, space-time, and BB84′ QKD protocols respectively. Fraction of the total resource distributed for various purposes (columns 2-5): Key (K):= For secret key bits generation, Test (T):= To test for eavesdropping, Discard (D):= Not used for anything, Wastage $(W = T + D)$:= Total amount of wastage [JSW⁺00]. N is the number of singlets ($|S_0\rangle$s) required to generate M bits of secret key ($M = NK$). CC:= Total amount of classical communication (in bits) required to generate M bits of secret key (see Sec. 6.4.3). $\mathcal{S}_m$ is the sensitivity to eavesdropping (Eq. (6.16)). First three QKD protocols are based on Bell's theorem. E:= requires an ensemble of large number of $|S_0\rangle$s to test for eavesdropping (see Secs. 6.4.1, 6.4.4 for explanation). $0 < \epsilon \ll 1/2$.

	K	T	D	W	N	CC	$\mathcal{S}_m$
Ek	$2/9$	$\frac{4}{9}$(E)	$\frac{3}{9}$	$7/9$	$\frac{9M}{2}$	14M	depends on m, and < 1
Wi	$1/4$	$\frac{3}{4}$(E)	0	$3/4$	$4M$	11M	depends on m, and < 1
ST	$\frac{1}{2} - \epsilon$	ϵ	$\frac{1}{2}$	$\frac{1}{2} + \epsilon$	$\frac{2M}{1-2\epsilon}$	$\frac{2M(3+\epsilon)}{1-2\epsilon}$	1
B′	$\frac{1}{2} - \epsilon$	ϵ	$\frac{1}{2}$	$\frac{1}{2} + \epsilon$	$\frac{2M}{1-2\epsilon}$	$\frac{2M(2+\epsilon)}{1-2\epsilon}$	-

Finally it is important to note that, one can also observe violation of Bell inequality greater than 2, and even upto its algebraic bound 4, due to loopholes (such as locality loophole, detection or fair-sampling loophole, using faked-state technique etc.) in performing the Bell test as well [GLLL⁺11, PSS⁺11, CZY⁺16]. However in this article, all our theoretical calculations are based on the assumption that there will not be any such loopholes in performing the Bell test. Hence the algebraic bound 4 which we were able to achieve, was not due to any kind of such loopholes. Further note that in our protocol, Alice and Bob are post-selecting with respect to their choice of measurement observables only, but not with respect to their measurement outcomes. In the ST-QKD protocol, Alice and Bob publicly announce their choice of measurement observables only, but not their measurement outcomes, and then post-select accordingly. Hence the violation of Bell inequality which Alice and Bob achieve (which is upto 4), is not due to fair-sampling loophole (this corresponds to post-selecting with respect to measurement outcomes [Bra11, CZY⁺16]). If it were so, then our protocol could not have been used for QKD.
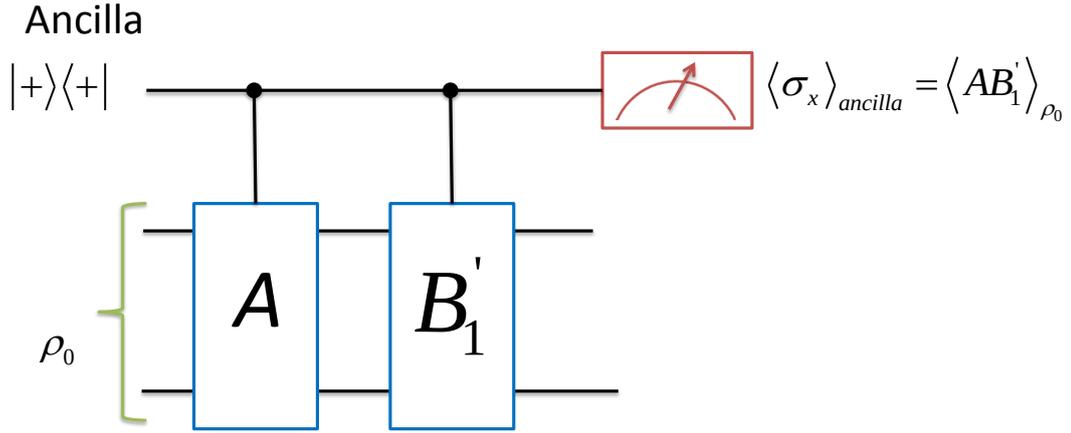
Fig. 6.1: Quantum circuit describing Moussa protocol to extract the expectation value $\langle AB'_1 \rangle_{\rho_0}$. Other three expectation values in Eq. (6.12) can be extracted in a similar fashion.

6.5 An NMR experimental proposal to test space-time Bell-CHSH protocol

Let $B'_1 = (U^{(2)}_{+y})^\dagger B U^{(2)}_{+y}$. Then one can verify that

$$\langle A(t^A) B_1(t^B) \rangle = \mathrm{Tr}(AB'_1 \rho_0) = \langle AB'_1 \rangle_{\rho_0} \tag{6.18}$$

and $B'_1 B'^\dagger_1 = B'_1 B'_1 = I \otimes I$. Similar relations hold for other three expectation values in Eq. (6.12) as well. Hence we can use Moussa protocol [MRCL10] in NMR to extract the expectation values, as shown in Fig. 6.1.

6.6   Summary and conclusion

We showed that if we insert context dependent local unitary evolutions into normal Bell test, then it is possible to violate space-time (ST) Bell-CHSH inequality maximally (i.e., up to 4). Correct context dependency can be achieved via post-selection. We presented a scheme to boost the correlation over space to the maximum extent possible (i.e., 4) via local unitary evolutions and subsequent classical communication (i.e., post-selection). This does not contradict Tsirelson bound $(2\sqrt{2})$, as the latter does not take into consideration unitary evolutions and/or post-selection. Further we showed that this leads to a more efficient and more sensitive (to eavesdropping) ST quantum key distribution (QKD) protocol. ST QKD protocol is far efficient and economical in terms of resource (singlets, classical communication) required to generate a given amount of secret key bits, than Ekert's and Wigner's QKD protocols. This can be achieved at the cost of introducing a simple local unitary evolution (i.e., ± 45 degree rotation about y-axis on the Bloch sphere). However compared to BB84' (i.e., modified BB84), ST QKD protocol is less efficient only in one aspect i.e., classical communication required, and in other aspects it is same as BB84'. We also showed that, when the amount of secret key bits to be generated is small, only ST and BB84' QKD protocols are economical.

Finally we note that if we get access to nonlinear evolution (closed time like curve based qubit) then BB84 becomes insecure [BHW09]. However entanglement monogamy may still ensure security of QKD via nonlocal correlation [Paw10]. In this sense entanglement based QKD might be more superior to BB84.

CHAPTER 7
Future directions

The standard text book quantum mechanics (QM) [CTDL05] is based on two pillars viz., postulates of QM, and A. N. Kolmogorov's mathematical model of quantum random phenomena (i.e., modern axiomatic, measure theoretic approach to the theory of random phenomena) [Gut05]. This gives rise to the widely used density matrix description in QM. Let us call this Kolmogorov QM (KQM). In chapter 5 we proposed a new mathematical model of quantum random phenomena, inspired by Richard von Mises [ST05, Ros10]. We call this Frequentist-inspired QM (FQM). As a potential application, superluminal communication which is prohibited in KQM (i.e., density matrix description), becomes possible in FQM. We believe that our new model FQM is an important step forward in the recent efforts elsewhere (see [PSCWH00, LZJ$^+$06, Pop18, GLTZ19]), to tackle many problems in QM, arising solely due to using density matrix description. FQM being a very fundamental revival in our understanding of the foundations of QM, we believe that it deserves further deeper investigation. In the following, we propose further line of research into FQM.

Note: All the expressions, notations, acronyms etc., referred below, correspond to chapters 4 and 5.

(1) Consider ineq. (8.29) which corresponds to procedure-A. Is there a way to eliminate linear terms in ineq. (8.29) and get only the quadratic terms in $\kappa(\cdots)$, by applying $R_x(X^\Theta)$ in some fashion? If we can do this, then we will get a clear reduction in fluctuation in procedure-A, compared to that in procedure-B.

(2) Can we formulate in a sensible way, procedure-B (because this is simple) as a random walk problem, and use the pathwise approach of mathematical finance [Son06] to predict the dynamics ?

(3) It appears that $\kappa(X = +1)$ corresponds to more than the measure zero set [Spa13, Wil10, Bil95] corresponding to $P(X = +1) = 1/2$. It requires further investigation. It will give us more insight into the connection between $\kappa(X = +1)$ and the measure zero set. Of course, the notion of measure zero set arises only when we assume *a priori* a constant value for probability of a random event. Hence measure zero set does not make sense in FQM. Still, looking for a connection may throw more light on the difference between the two approaches viz., KQM and FQM.

(4) Strong LLN says, limiting relative frequency $\lim_{N \to \infty} N_{+1}(X, N)/N$ converges almost surely, but not surely (even though convergence happens with probability one), to $1/2$. This is because of non-empty measure zero set (it is infinitely large). But 'almost' is just a qualitative statement [Spa13]. This is because, does 'almost sure' mean 99.99% or 99.999% or ...? We may have to look into the law of iterated logarithms for a quantitative statement about convergence [Spa13].

(5) It appears that there is some connection between justification of measure theoretic approach via strong LLN and Gödel's incompleteness theorem [Raa18, Pen06]. A mathematically rigorous investigation from this perspective will shed more light on the measure theory of Kolmogorov.

(6) In reality we cannot realize $N \to \infty$, even though it is possible in principle/conceptually. Hence the case $1 \ll N < \infty$ requires more investigation, because this is what we can realize in a real experiment.

(7) In KQM we have an averaged measure of fluctuation (because all quantities are weighed using the *a priori* assumed probabilities, and it cannot capture fundamental

fluctuation). Whereas in FQM we have fluctuations in-itself. Further investigation into this will give more insight into the differences between the two approaches.

(8) To look for a deeper connection between Knightian uncertainty and $\kappa(X = +1)$.

(9) Boltzmann entropy is based on frequentist-inspired or pathwise approach to random phenomena whereas von Neumann entropy is based on density matrix description [GLTZ19]. In non-equilibrium, only Boltzmann entropy gives correct prediction which is in accordance with second law of thermodynamics [GLTZ19]. To carry out further investigation into it, because it may throw more light on the differences between the two incompatible approches viz., KQM and FQM.

(10) Postulates of quantum mechanics + Frequentist-inspired approach to random phenomena $= - - - - - - -$ description (i.e., what plays the role of density matrix in FQM?; In FQM, is there a mathematical object analogous to density matrix?)

(11) It may be possible to test the predictions of FQM via spin noise in NMR.

(12) We need to reanalyze the problem of whether there is entanglement in NMR systems at room temperature [LZJ$^+$06], in the new light of FQM. Then it may turn out, within FQM, that even entanglement is contributing to the QFI amplification shown in chapter 4. Also the problem of spin noise in NMR wherein we get signal due to incomplete statistical cancellation, even if we do not use radio frequency pulse to tilt thermal equilibrium magnetization along z-axis onto x-y plane, in the Bloch sphere representation [Blo46, FHLD15].

(13) It is the entanglement and the nonlinear collapse dynamics of quantum measurement which is the main resource for signaling. FQM's discrimination protocol just decodes the already superluminally transferred information. Our protocol shows that signaling is in principle possible. Hence it motivates us to search for better signaling resources like PT-symmetric nonunitary quantum mechanics [LHFL14], exploiting the

time of nonlinear wave function collapse dynamics etc.

(14) Is there a connection between nonlinear dynamics of quantum measurement (collapse) and signaling, and hence solution of NP and #P problems in polynomial time [AL98, LHFL14], and also with cloning an arbitrary unknown quantum state?

(15) How can we reconcile the signaling predicted within FQM with special relativity [LSV02, Fei67]? One can show that it is possible to encode information onto linear polarization degree of freedom of a photon in such a fashion that the amount of gravitational red shift of the photon is unaffected. This shows that information carries no mass and/or linear momentum. Instead of linear polarization if we consider circular polarization degree of freedom of a photon to encode information, then it might be possible to show (via something which is sensitive to angular momentum) that information carries no angular momentum as well. Then it implies that information is not physical. (This result will be published elsewhere.)

However information has to be encoded in a physical observable like spin angular momentum. Hence violation of Bell inequality and subsequent signaling predicted within FQM, implies an instantaneous change in spin angular momentum (and hence energy distribution) across spacelike separation. This is the dynamical aspect of Bell nonlocality. Note that even in Aharonov-Bohm effect there is an instantaneous change in kinetic energy distribution of an electron across spacelike separation [AB59, AK04, ACR16]. This can be reconciled with special relativity provided there exists an underlying quantum nonlocal field from which quanta of spacetime (gravitational field [Rov04]) and matter (matter field) emerge as a consequence of nonlocal field excitation. And special relativity holds within spacetime only. (Research along these lines is under progress.)

(16) It is interesting to discuss the unknown parameter estimation using QFI when the ancillary qubits are classically correlated with the target qubit. For this purpose we may proceed as follows: Consider states in which target and ancillary qubits are not

even classically correlated. Then calculate QFI (corresponding to SLD). Next consider states in which target and ancillary qubits are only classically (pre)correlated but have no quantum (pre)correlations like quantum discord, entanglement etc. (For this purpose we may use the results of [KLKW18].) Then find QFI (again corresponding to SLD) and see if there is an enhancement compared to the previous one.

CHAPTER 8

Appendix

8.1 Postulates of theory of random phenomena are independent of postulates of QM

It is very important to carefully and clearly distinguish between axioms/postulates of QM and the axioms of mathematical model of random phenomena which is necessary to analyze the post measurement data and/or predict (stochastically but not deterministically) the outcome of even a single projective measurement. The collapse of the state vector postulate of QM do not say anything about which theory/mathematical model of random phenomena is to be used. Born's probabilistic interpretation of state vector uses Kolmogorov's modern axiomatic probability measure theory of random phenomena and the resulting QM is known as density matrix description or KQM or standard QM i.e.,

$$\text{Postulates of QM} + \text{Kolmogorov's probability measure theory}$$
$$= \text{density matrix description or KQM.}$$
$$\text{Postulates of QM} + \text{frequentist inspired theory ofrandom phenomena} = \text{FQM.} \quad (8.1)$$

FQM is based on an alternate approach to the theory of random phenomena which is motivated by experiment (i.e., operationally motivated) and hence do not assume *a priori* a probability measure unlike in KQM. FQM uses *a posteriori* LRF instead of *a*

priori probability measure.

8.2 Fundamental difference between von Mises definition of probability (and hence FQM's LRF) and Kolmogorov's *a priori* probability

The basic, fundamental, and crucial difference between von Mises definition of probability (and hence FQM's definition of LRF) and Kolmogorov's *a priori* assumption of a constant value for the probability of a *single* random event is the following.

von Mises defined probability as

$$P(X = +1) = \lim_{N \to \infty} N_{+1}(X, N)/N = 1/2 \tag{8.2}$$

(see [Ros10] in this regard). von Mises assumed that the limit always exists but it is not correct as shown in Appendix 8.9, and hence $\kappa(X = +1)$ term comes into picture. That is, in FQM, LRF of the event $X = +1$ is defined as

$$F(X = +1) := \limsup_{N \to \infty} \frac{N_{+1}(X, N)}{N} = \frac{1}{2} + \kappa(X = +1). \tag{8.3}$$

This is based on relative frequency and hence requires an ensemble or repetition of the experiment, under identical conditions, a large number of times. Whereas Kolmogorov assumed *a priori* a constant value (a real number between 0 and 1) for the probability of a single random event [Gut05] (but not an ensemble) i.e.,

$$P(X = +1) = 1/2. \tag{8.4}$$

110

A priori probability is based on an observer's intuitive/subjective notion like "equally likely" events. It is an abstract mathematical quantity. It has no direct connection with actual random phenomena (i.e., experiment) but it may be interpreted as an observer's subjective measure of belief [Ros10, GLTZ19] that in a single trial of X the outcome will be $+1$. *A priori* probability per se has nothing to do with/has no connection with outcomes of a large number of trials of random variable(s) i.e., an ensemble. (In fact the notion of probability measure started with gambling like casino, dice throw etc., where we are forced to predict probabilistically, but not deterministically, the outcome of a single trial of a random variable.) E.g., let Alice prepare a single qubit in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Then according to KQM, the state of the single qubit from Alice's perspective is described/represented by the pure density matrix

$$\rho = |+\rangle\langle+|. \tag{8.5}$$

(Whereas the state of an ensemble of $\mathcal{M}$ number of identical copies of $|+\rangle$ is represented by $\rho^{\otimes\mathcal{M}}$.) Let Alice measure the observable $|0\rangle\langle0|$ on ρ. Then density matrix description predicts probabilistically (but not deterministically) that Alice will obtain a single outcome $+1$ with *a priori* assumed probability $1/2$ (Born's probabilistic interpretation of state vector) i.e.,

$$P(X = +1) = \text{Tr}(|0\rangle\langle0|\rho) = 1/2. \tag{8.6}$$

We may interpret, connect, and justify *a priori* probability $1/2$ (and hence ρ) using an ensemble of identical copies of $|+\rangle$, in some sense, for practical purposes only (see Appendix 8.2.1). But strictly speaking, fundamentally *a priori* probability pertains only to a single copy of $|+\rangle$. This follows from the very meaning of *a priori* assumption. If it is not so, then *a priori* assumption becomes pointless and meaningless (also see Appendices 8.9.2, 8.2.2).

All the above notions and points apply to mixed states as well e.g., in the above example assume that Bob knows everything except Alice's outcome of measuring $|0\rangle\langle0|$ on $|+\rangle$. Then according to density matrix description or KQM, the average state of a single qubit (but not an ensemble of qubits each prepared using the same preparation procedure) from Bob's perspective is described by the mixed density matrix

$$\rho^B = (|0\rangle\langle0| + |1\rangle\langle1|)/2. \tag{8.7}$$

Mixedness here is a measure of Bob's subjective ignorance about the state of the given single qubit. In other words ρ^B is psi-epistemic (but not psi-ontic) i.e., ρ^B represents an observer's state of knowledge (or amount of ignorance) about the state of the given single qubit [WB12, AAP11].

However if Bob wants to consider the actual physical state of the given single qubit path by path then he must drop the *a priori* assumption of a probability measure associated with Alice's $|0\rangle\langle0|$ measurement outcome, as done in FQM. Here it is important to note that the two notions viz., path by path and *a priori* probability measure cannot coexist simultaneously. Presence of one excludes the other. If we assume *a priori* a probability measure then we are forced to consider the average state. This is why FQM and KQM are fundamentally incompatible.

8.2.1 Physical justification, in some sense, for practical purposes, of *a priori* probability: Connection with an ensemble

Kolmogorov's strong LLN tries to establish connection between theory (*a priori* assumed probability measure) and experiment (limiting relative frequency), and hence it tries to

give an experimental justification, in some sense, for the *a priori* theoretical probability. Convergence shown by Kolmogorov's strong LLN is in terms of the very notion which it is actually trying to define/explain/justify i.e., probability, but not pointwise convergence [ST05]. That is, Kolmogorov's strong LLN shows that [Ros10]

$$P(\lim_{N\to\infty} N_{+1}(X,N)/N = 1/2) = 1, \tag{8.8}$$

and it is known as almost sure (but not 100% sure) convergence because there is infinitely large measure zero set [Wil10]. Given the definition and nature of random phenomena, $\kappa(X = +1)$ term follows (see Eq. (8.3)) upon dropping the *a priori* assumption of a probability measure and using LRF (which do not converge pointwise to 1/2 always, as shown in Appendix 8.9) instead of a probability measure. However for most of the practical purposes, whenever $N \gg 1$, we may safely neglect $\kappa_N(X = +1)$ i.e.,

$$\text{for } N \gg 1, \ N_{+1}(X,N)/N \approx 1/2. \tag{8.9}$$

This has ample experimental evidence as well (i.e., stabilization of relative frequency [Gut05]). This is the sense in which predictions of Kolmogorov's strong LLN has been tested experimentally. This is also the sense in which the predictions of KQM has been verified experimentally so far (also see example-A discussed below). But FQM is pointing to an experiment (discriminating between two different ensemble preparation procedures discussed in chapter 5) wherein we may observe deviation from the predictions of KQM. Examples discussed by Popescu [Pop18], Goldstein et. al. [GLTZ19] etc., also fall in this category.

Example-A

Consider measuring σ_z on a single copy of $|+\rangle$. Then according to KQM, $\rho = |+\rangle\langle+|$ and $\langle\sigma_z\rangle_\rho = \mathrm{Tr}(\sigma_z\rho) = 0$. This is nothing but theoretical mean value of the observable σ_z based on observer's measure of belief (which is 1/2) that single outcome of σ_z measurement will be $+1$ and observer's measure of belief (1/2) that single outcome of σ_z measurement will be -1 i.e., $\langle\sigma_z\rangle_\rho = 1/2 \times (+1) + 1/2 \times (-1) = 0$. When $P(\sigma_z(\rho) = \pm 1) = 1/2$ correspond to a single measurement outcome, then how come $\langle\sigma_z\rangle_\rho$ (which is based on $P(\sigma_z(\rho) = \pm 1) = 1/2$) not correspond to a single measurement outcome? Let $S_N = (1/N)\sum_{i=1}^{N}\sigma_{zi}$ where σ_{zi} is the outcome of σ_z measurement on i-th copy of $|+\rangle$. Kolmogorov's strong LLN tries to justify/connect the theoretical mean $\langle\sigma_z\rangle_\rho = 0$ to experimental observation via $P(\lim_{N\to\infty} S_N = 0) = 1$. But the convergence is not pointwise. And what we actually observe is $\lim_{N\to\infty} S_N$ and it will not always converge pointwise to 0 (Appendix 8.9). And hence we have, in FQM, $\lim_{N\to\infty} S_N = 2\kappa(\sigma_z(|+\rangle) = +1)$. But for most of the practical purposes, we may safely neglect $\kappa_N(\sigma_z(|+\rangle) = +1)$ where $N \gg 1$, and say that theoretical mean value predicted by ρ has been realized experimentally. In this approximate sense, we may associate/connect ρ with an ensemble and answer questions about average properties also pertaining to an ensemble. But from a foundational point of view, we cannot neglect $\kappa(\sigma_z(|+\rangle) = +1)$, and ρ describes state of a single qubit and answers questions about mean values also pertaining to a single qubit's state (but not an ensemble of identical qubit states). In fact it is the FQM which fundamentally answers questions about average properties pertaining to an ensemble only, without assuming *a priori* a probability measure.

In the preceding calculations if we replace ρ by $\rho^B = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2$ then from foundational point of view, ρ^B describes average (but not actual) state of a single qubit and answers questions about mean values also pertaining to a single qubit (but not an

ensemble of qubits).

8.2.2 *A priori* probability measure corresponds to a single random event but not an ensemble

There are certain random phenomena which are not repeatable (or we are not allowed to repeat) e.g., horse race, insurance company, gambling (casino, dice throw etc). In such situations we are forced to predict (not deterministically but only stochastically or probabilistically) outcome of a single trial of the random variable. There are many approaches to tackle this problem viz., Kolmogorov's modern axiomatic probability measure theoretic approach [Gut05] which assumes *a priori* a constant value (a real number between 0 and 1) for the probability of a single random event i.e., assumes *a priori* a probability measure; Pathwise approach [Son06] (used in mathematical finance to handle Knightian uncertainty) which do not assume *a priori* a probability measure; Imprecise probability approach [VS12] etc. FQM cannot make any prediction in such cases as it do not assume *a priori* a probability measure and as it requires an ensemble i.e., a large number of trials of the given random variable(s) to make any predictions which are based on $\kappa(.)$ terms.

Even if we repeat the experiment infinitely many times still we can never be 100% sure of obtaining/observing 1/2 because relative frequency cannot always converge pointwise to 1/2 (see Appendix 8.9). Then how come *a priori* probability 1/2 (and hence ρ) is associated not with a single measurement outcome but is associated with a large number of measurement outcomes/ensemble? The very meaning of the axiom (i.e., assuming *a priori* a real number between 0 and 1 for the probability of a single random event) itself clearly shows that *a priori* probability 1/2 pertains/corresponds to a single random event but not an ensemble. (Note that probability one implies sure occurrence provided

measure zero set is empty. E.g., in case of Kolmogorov's strong LLN, measure zero set is infinitely large and hence the convergence shown by Kolmogorov's strong LLN is almost sure but not 100% sure convergence.) Kolmogorov's strong LLN tries to justify, in some sense, the *a priori* assumed probability 1/2 (which is subjective) by connecting it with experiment i.e., limiting relative frequency (which is objective).

If *a priori* probability requires an ensemble framework i.e., a large number of measurement outcomes to justify/obtain it, then *a priori* assumption of a probability measure becomes pointless and meaningless. The very meaning of *a priori* is, no connection with experiment. It is the FQM which requires an ensemble framework to obtain LRF (which plays the role of KQM's *a priori* probability measure) because FQM do not assume *a priori* a probability measure. In fact it is the FQM which fundamentally answers questions about average properties pertaining to an ensemble only (but not a single qubit) without assuming *a priori* a probability measure.

A priori probability 1/2 is an abstract mathematical (theoretical) quantity which may be connected, in some sense, with experiment, as shown above. We may interpret it as an observer's subjective measure of belief that the outcome in a single trial of X will be $+1$.

8.2.3 FQM v/s KQM: Known and unknown states

KQM or standard QM: Known or partially known or completely unknown state of a single qubit is described by density matrix which lives in operator space (but not in Hilbert space) which allows incoherent superposition (e.g., $(|0\rangle\langle0| + |1\rangle\langle1|)/2$ is an incoherent superposition as it do not give rise to any interference effects between its two components viz., $|0\rangle\langle0|$ and $|1\rangle\langle1|$ [Aud07]).

$\rho^B = (|0\rangle\langle0| + |1\rangle\langle1|)/2$ describes the average state of a single qubit whereas $\rho^{B^{\otimes\mathcal{M}}}$

116

describes average state of an ensemble of $\mathcal{M}$ number of identically prepared qubits.

When we have full information about the state of a single qubit (i.e., state is known) then its state is described by either a state vector living in Hilbert space (FQM) or a pure density matrix living in operator space (KQM). When we have partial information about the state of a single qubit (i.e., state is unknown) then its state is described by either a set of state vectors living in Hilbert space without assuming *a priori* a probability measure for the stochastic process used to prepare the unknown state (FQM, quantum teleportation, proof of nocloning theorem, BB84 etc.) or a mixed density matrix living in operator space (KQM).

It is important to note that $\kappa(.,.)$ is not the only difference between FQM and KQM. E.g., in quantum teleportation, approximate cloning, BB84, discriminating between linearly dependent and independent state vectors etc. (see Sec. 5.4), $\kappa(.,.)$ terms are not used at all but one considers all possible states corresponding to the given unknown quantum state, path by path, without assuming *a priori* a probability measure for the stochastic process used to prepare the single copy of the given unknown quantum state. $\kappa(.,.)$ terms are necessary if we are interested in fluctuation. Crucial and fundamental difference between KQM and FQM is in assuming *a priori* a probability measure. $\kappa(.)$ is a natural consequence of dropping *a priori* assumption of a probability measure.

8.3   QST propagator U_T in N-qubit STR

The task of the QST operator U_T (eq. (4.11)) is to transfer information about the state of the target qubit onto the ancillary qubits. Motivated from the INEPT sequence, we modeled this operator in the form

$$U_T = U_{\theta_2^t, \phi_2^t} U_{J, \tau_2} U_{\theta_1^t, \phi_1^t} U_{\theta_2^a, \phi_2^a} U_{J, \tau_1} U_{\theta_1^a, \phi_1^a}, \tag{8.10}$$

117

where

$$U_{\theta_j^{a/t}, \phi_j^{a/t}} = e^{-i\theta_j^{a/t}\left(I_x^{a/t}\cos\phi_j^{a/t} + I_y^{a/t}\sin\phi_j^{a/t}\right)}, \tag{8.11}$$

with $I_\alpha^a = I_{0\alpha}^A + I_{1\alpha}^A$ (see eq. (4.10)), $I_\alpha^t = I_{1\alpha}$ (eq. (4.5)) for $\alpha \in \{x, y, z\}$, $\theta_j^{a/t}$ is the nutation angle, $\phi_j^{a/t}$ is the phase, and

$$U_{J,\tau_j} = e^{-i\pi J\tau_j 2I_{1z}I_z^a}. \tag{8.12}$$

Using these parameters $\{\theta_j^{a/t}, \phi_j^{a/t}, \tau_j\}$ we can now construct the constraint matrix Z by applying eqs. (4.11). We optimized these parameters using the genetic algorithm routine of MATLAB, and obtained the solution illustrated in fig. 4.1(d). While the solution is not unique, we found it to be sufficient for our purposes.

8.4 Constraint Matrix Z

Constraint matrix Z (eq. (4.12)) corresponding to the U_T given in fig. 4.1(d) is the following

$$Z = \begin{bmatrix} 1.5222 & -2.3043 & 1.2564 \\ -0.5025 & -1.3001 & 1.9377 \\ 2.1985 & -1.4165 & 2.3981 \\ 1.5946 & 0.2081 & -1.3022 \end{bmatrix}, \tag{8.13}$$

whose condition number is 4.5, which is sufficiently low for practical purposes. One of our experimental signals was

$$
S = \begin{bmatrix} \langle I_{0x}^A \rangle \\ \langle I_{0y}^A \rangle \\ \langle I_{1x}^A \rangle \\ \langle I_{1y}^A \rangle \end{bmatrix} = \begin{bmatrix} -2.1956 \\ -1.4463 \\ -1.3123 \\ 0.2762 \end{bmatrix}. \tag{8.14}
$$

Using eq. (4.12), we now find

$$
\begin{bmatrix} \sin\theta_0 \cos\phi_0 \\ \sin\theta_0 \sin\phi_0 \\ \cos\theta_0 \end{bmatrix} = Z^{-1} S = \begin{bmatrix} 0.0657 \\ 0.9976 \\ -0.0218 \end{bmatrix}, \tag{8.15}
$$

which leads to $(\theta_0, \phi_0) = (1.01\pi/2, 0.96\pi/2)$ and the corresponding correlation with $(\pi/2, \pi/2)$ is 99.8 as mentioned in the Table 4.1.

8.5 QFI of a single-qubit

8.5.1 Polar parameter

Consider eq. (4.16). Since the partial derivative

$$
\frac{\partial \varrho_{\theta,\phi_0}}{\partial \theta} = \frac{\varepsilon_{t,1}}{2} \begin{bmatrix} -\sin\theta & e^{-i\phi_0}\cos\theta \\ e^{i\phi_0}\cos\theta & \sin\theta \end{bmatrix} = \frac{\varepsilon_{t,1}}{2} \frac{\partial \hat{n}}{\partial \theta}.\vec{\sigma}, \tag{8.16}
$$

119

the corresponding unbiased observable for a single target qubit turns out to be (using eqs. (4.3) and (4.17)) [ZSM$^+$13]

$$M_{\overleftrightarrow{\theta_0},\phi_0} = 2 \left.\frac{\partial \varrho_{\theta,\phi_0}}{\partial \theta}\right|_{\theta_0} = \varepsilon_{t,1} \left.\frac{\partial \hat{n}}{\partial \theta}\right|_{\theta_0}.\vec{\sigma}. \tag{8.17}$$

Since $\hat{n}_0. \left.\frac{\partial \hat{n}}{\partial \theta}\right|_{\theta_0} = 0$, the unbiased observable corresponds to a direction orthogonal to the target state $\varrho_{\theta_0,\phi_0}$.

Often the measurement observable is not the same as the optimal (unbiased) observable. For example, a QST observable makes no prior assumption about the target state, and hence is in general a biased observable. To study QFI under a biased observable, we now consider a deviation of a chosen observable from the optimal observable (eq. (8.17)) via $\Theta_0 = \theta_0 + \delta\theta_0$ and $\Phi_0 = \phi_0 + \delta\phi_0$. The chosen (or biased) observable is of the form

$$M_{\overleftrightarrow{\Theta_0},\Phi_0} = \varepsilon_{t,1} \begin{bmatrix} -\sin\Theta_0 & e^{-i\Phi_0}\cos\Theta_0 \\ e^{i\Phi_0}\cos\Theta_0 & \sin\Theta_0 \end{bmatrix}. \tag{8.18}$$

QFI obtained using eq. (4.13) is then

$$F_\theta(\varrho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\Theta_0},\Phi_0}) = $$
$$\frac{\varepsilon_{t,1}^2(\cos\delta\phi_0\cos\theta_0\cos\Theta_0 + \sin\theta_0\sin\Theta_0)^2}{1 - \varepsilon_{t,1}^2(\cos\delta\phi_0\sin\theta_0\cos\Theta_0 - \cos\theta_0\sin\Theta_0)^2}.$$

For $\delta\phi_0 = 0$ we obtain

$$F_\theta(\varrho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\Theta_0},\phi_0}) = \frac{\varepsilon_{t,1}^2\cos^2\delta\theta_0}{1 - \varepsilon_{t,1}^2\sin^2\delta\theta_0}. \tag{8.19}$$

fig. 8.1 displays the profile of QFI in the above scenario. For the maximally biased observable with $\delta\theta_0 = \pi/2$, QFI vanishes throughout, while for the optimal case, with
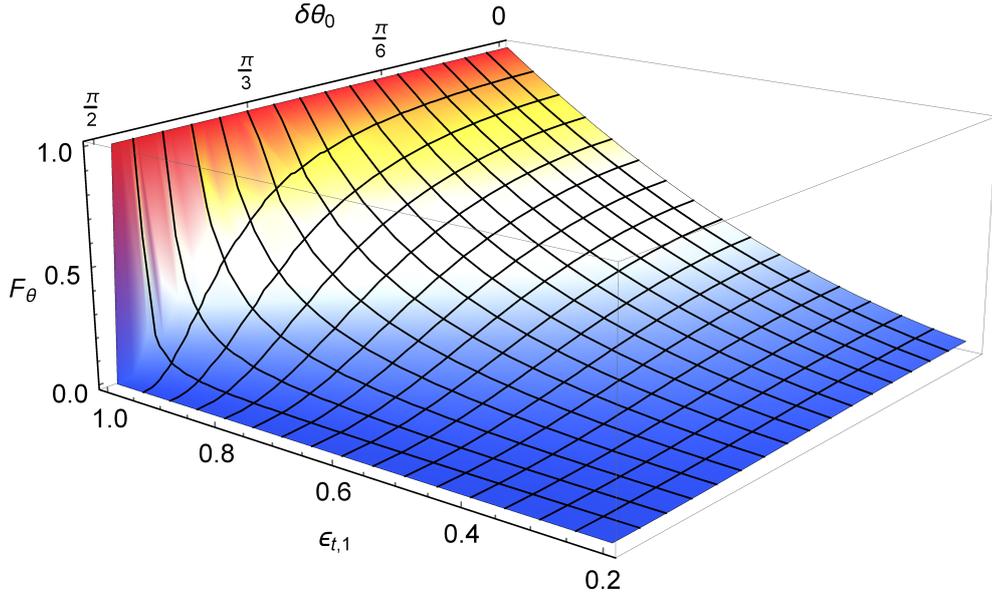
Fig. 8.1: Profile of QFI F_θ versus the deviation $\delta\theta_0$ in the polar angle and the generalized Bloch radius $\varepsilon_{t,1}$, as described by eq. (8.19).

$\delta\theta_0 = 0$ we obtain the upper bound $\varepsilon_{t,1}^2$ for the mixed state QFI (see eq. (4.19)).

8.5.2 Azimuthal parameter

Consider eq. (4.21). Since $\hat{n}_0 \cdot \frac{\partial \hat{n}}{\partial \phi}\big|_{\phi_0} = 0$, to achieve optimal measurement one has to measure in a direction orthogonal to the state $\varrho_{\theta_0,\phi_0}$. Hence the directions $\hat{n}_0$, $\frac{\partial \hat{n}}{\partial \theta}\big|_{\theta_0}$, and $\frac{\partial \hat{n}}{\partial \phi}\big|_{\phi_0}$ are mutually orthogonal. Again, we consider a deviation of a chosen observable from the optimal observable (eq. (4.21)) via $\Theta_0 = \theta_0 + \delta\theta_0$ and $\Phi_0 = \phi_0 + \delta\phi_0$, and the corresponding biased observable is then

$$M_{\Theta_0,\overleftrightarrow{\Phi_0}} = \varepsilon_{t,1} \sin\Theta_0 \begin{bmatrix} 0 & -ie^{-i\Phi_0} \\ ie^{i\Phi_0} & 0 \end{bmatrix}. \tag{8.20}$$

QFI obtained using eq. (4.14) is then

$$F_\phi(\varrho_{\theta_0,\phi_0}, M_{\Theta_0,\overleftrightarrow{\Phi_0}}) = \frac{\varepsilon_{t,1}^2 \cos^2 \delta\phi_0 \sin^2 \theta_0}{1 - \varepsilon_{t,1}^2 \sin^2 \delta\phi_0 \sin^2 \theta_0},$$

which is independent of $\delta\theta_0$. For the unbiased observable (SLD) i.e., $\delta\theta_0 = \delta\phi_0 = 0$, we obtain eq. (4.22).

8.6 Why is the simultaneous estimation of (θ, ϕ) not possible?

Simultaneous estimation of both the parameters θ and ϕ is not possible as they are not compatible for the following reason. Consider $F_\theta(\varrho_{\theta_0,\phi_0}, M_{\overleftrightarrow{\theta_0},\phi_0})$ and $F_\phi(\varrho_{\theta_0,\phi_0}, M_{\theta_0,\overleftrightarrow{\phi_0}})$ (sec. 4.4.1). These QFIs correspond to individual estimation of θ, ϕ. However if the SLDs $M_{\overleftrightarrow{\theta_0},\phi_0}$ and $M_{\theta_0,\overleftrightarrow{\phi_0}}$ commute, then we can measure in the common eigenbasis and estimate both θ, ϕ simultaneously, and still achieve same precision as in individual estimation scenario [RJDDan16]. This saves resource. However the compatibility of SLDs is sufficient but not necessary for simultaneous estimation [RJDDan16]. Weaker conditions necessary for simultaneous estimation are the following:

$$\begin{aligned}
\mathrm{Im}(\mathrm{Tr}(\varrho_{\mu,\nu}AB)) &= 0 \ \forall \ A, B \text{ and} \\
\mathrm{Re}(\mathrm{Tr}(\varrho_{\mu,\nu}AB)) &= 0 \text{ for } A \neq B,
\end{aligned} \tag{8.21}$$

where $A, B \in \{M_{\overleftrightarrow{\mu},\nu}, M_{\mu,\overleftrightarrow{\nu}}\}$ [YNSA17]. However in our case,

$$
\begin{aligned}
\mathrm{Im}(\mathrm{Tr}(\varrho_{\theta_0,\phi_0} M_{\overleftrightarrow{\theta_0},\phi_0} M_{\theta_0,\overleftrightarrow{\phi_0}})) &= -\mathrm{Im}(\mathrm{Tr}(\varrho_{\theta_0,\phi_0} M_{\theta_0,\overleftrightarrow{\phi_0}} M_{\overleftrightarrow{\theta_0},\phi_0})) = \varepsilon_{t,1}^3 \sin\theta_0, \\
\mathrm{Im}(\mathrm{Tr}(\varrho_{\theta_0,\phi_0} M_{\overleftrightarrow{\theta_0},\phi_0}^2)) &= \mathrm{Im}(\mathrm{Tr}(\varrho_{\theta_0,\phi_0} M_{\theta_0,\overleftrightarrow{\phi_0}}^2)) = 0, \\
&\text{and}
\end{aligned}
$$

$$
\mathrm{Re}(\mathrm{Tr}(\varrho_{\theta_0,\phi_0} M_{\overleftrightarrow{\theta_0},\phi_0} M_{\theta_0,\overleftrightarrow{\phi_0}})) = \mathrm{Re}(\mathrm{Tr}(\varrho_{\theta_0,\phi_0} M_{\theta_0,\overleftrightarrow{\phi_0}} M_{\overleftrightarrow{\theta_0},\phi_0})) = 0.
$$

Hence the incompatible parameters (θ, ϕ) cannot be estimated simultaneously.

8.7 QFI with quadrature measurement

Single qubit case: We define the analog of dual parameter quantum Cramer-Rao bound

$$
(\Delta\theta)^2 + (\Delta\phi)^2 \geq \inf\left\{\frac{1}{(k/2)F_\theta(\varrho'_{\theta_0,\phi_0}, I_\alpha)}\right\} + \inf\left\{\frac{1}{(k/2)F_\phi(\varrho_{\theta_0,\phi_0}, I_\alpha)}\right\} = \frac{1}{2k\mathbb{F}_Q(\varrho_{\theta_0,\phi_0})}
\tag{8.22}
$$

where infimum is over $\alpha \in \{x, y\}$. In a given quadrature detection, we have $k/2$ number of I_x measurements (real signal) and $k/2$ number of I_y measurements (imaginary signal). $2k$ in the denominator is because of using two quadrature detections (sec. 4.3.1). $F_\phi(\varrho_{\theta_0,\phi_0}, I_\alpha)$ is estimated using eq. (4.14). However, the θ_0 measurement involves destroying coherences using a PFG followed by an I_z measurement. In NMR, I_z measurement can be achieved by applying a $(\pi/2)_y$ pulse (i.e., nutation angle $\pi/2$, and phase $\pi/2$) on the state followed by an I_x measurement. This allows us to estimate $F_\theta(\varrho_{\theta_0,\phi_0}, I_z) = F_\theta(\varrho'_{\theta_0,\phi_0}, I_x)$ using eq. (4.13). Accordingly dual parameter quadrature QFI $\mathbb{F}_Q(\varrho_{\theta_0,\phi_0})$ is as given in eq. (4.36).

STR case: Similar to eq. (8.22) we define the analog of dual parameter quantum

Cramer-Rao bound as

$$(\Delta\theta)^2 + (\Delta\phi)^2 \geq \inf\{\frac{1}{(k/4)F_\theta(\rho_{\theta_0,\phi_0}, M_{q\alpha})}\} + \inf\{\frac{1}{(k/4)F_\phi(\rho_{\theta_0,\phi_0}, M_{q\alpha})}\} = \frac{1}{k\mathbb{F}_Q(\rho_{\theta_0,\phi_0})} (8.23)$$

where infimum is over $q \in \{0,1\}$ and $\alpha \in \{x,y\}$. Here we use single quadrature detection of ancillary qubits where each of the four observables $M_{q\alpha}$ is measured on $k/4$ copies of ρ_{θ_0,ϕ_0}. Hence there is k in the denominator. Accordingly we obtain dual parameter quadrature QFI $\mathbb{F}_Q(\rho_{\theta_0,\phi_0})$ as given in eq. (4.38).

8.8 In $F(X = +1)$, $1/2$ cannot be preferred over $1/2+c$

In Eq. (5.1), choosing $1/2$ is motivated/guided by the following factors: Experimental observation (i.e., stabilization of relative frequency [Gut05] somewhere around $1/2$), symmetry i.e., $|+\rangle$ is an equal superposition of the two eigenvectors of the observable being measured (i.e., $|0\rangle\langle 0|$), and convenience i.e, $1/2$ is the square of the Fourier coefficient or amplitude in $|+\rangle$. However from foundational point of view, these are not compelling and sufficient reasons to prefer $1/2$ over $1/2 + c, |c| > 0$. (Note that if we choose $1/2 + c$ then we will not recover KQM from FQM by setting $\kappa(.,.)$ terms to zero. But that is okay because any way in KQM, probability $1/2$ is an *a priori* assumption which is not based on experiment. Then there is no compelling reason for not to choose $1/2 + c$ (instead of $1/2$) as *a priori* probability.) The fact that $F(X = +1)$ cannot always converge pointwise to $1/2$ proves that even $F(X = +1)$ has intrinsic fluctuation. Further even if we repeat infinitely many times the experiment involving $N \to \infty$ number of trials of X, still $F(X = +1)$ may not always fluctuate symmetrically about $1/2$. This is more appealing in case of $F(X^{\theta \neq \pi/2} = +1)$ where X^θ is defined in the text preceding Eq. (5.4). This is due to fundamental uncertainty/indeterminacy arising due to intrinsic randomness in measurement outcomes. If $F(X = +1)$ would

124

always fluctuate symmetrically about 1/2 then that would contradict the very meaning, nature, and definition of random phenomena. What really matters and one can talk of is the relative fluctuation i.e., fluctuation of $F(X^{\theta=\pi/2} = +1)$ will be different compared to that of $F(X^{\theta\neq\pi/2} = +1)$. This is unlike in KQM wherein one can talk of absolute fluctuation due to the presence of quantitatively precise probability measure.

Of course we can absorb c into $\kappa(X = +1)$. But here we are trying to argue that $F(X = +1)$ may not always fluctuate symmetrically about 1/2. And hence there is no compelling reason to prefer 1/2 over $1/2 + c$.

8.9 No pointwise convergence of limiting relative frequency

If $\lim_{N\to\infty} N_{+1}(X,N)/N = 1/2$, then it implies that $\forall 0 < \epsilon < 1/2, \exists M < \infty$ such that $\forall N > M, |N_{+1}(X,N)/N - 1/2| < \epsilon$. However, as $N < \infty$, all possible outcomes will be realised with nonzero (positive) chance or possibility or likeliness, upon repeating the experiment many times. Hence the requirement for pointwise convergence to 1/2 is not always satisfied (e.g., for $N_{+1}(X,N) = N$).

8.9.1 For most of the practical purposes $\lim_{N\to\infty} N_{+1}(X,N)/N \approx 1/2$: Overlooks content dependent fluctuation

As N increases, the number of elements in the sample space which correspond to or give $N_{+1}(X,N)/N = 1/2$ also increases (also it is the highest for N even). Whereas there will always be only one element which gives $N_{+1}(X,N)/N = 1$ or 0. But as long as M, N are finite (however large), if we repeat sufficiently many times the experiment involving M or N trials each, then certainly we will obtain/realize even the element which gives

$N_{+1}(X, N)/N = 1$ or 0. Hence $\lim_{N \to \infty} N_{+1}(X, N)/N$ cannot always converge pointwise to 1/2. However for any given $\epsilon > 0$ we can choose M so large that for most of the practical purposes the condition $|N_{+1}(X, N)/N - 1/2| < \epsilon$ is almost always satisfied (this is an experimental fact i.e., stabilization of relative frequency [Gut05]). And hence we may say that $\lim_{N \to \infty} N_{+1}(X, N)/N \approx 1/2$ for most of the practical purposes. But by this approximation we miss out, overlook the existence of $\kappa(X = +1)$ term (Eq. (8.3)) and hence the content dependent fluctuation which is the key resource to distinguish between z and x ensembles i.e., $\mathcal{E}_A$ and $\mathcal{E}_B$. If content dependent fluctuation is present even in the limit $N \to \infty$, then it is justifiable to assume that it should be present even at large but finite N as well (because physics is the same at all N). Hence the above approximation misses out content dependent fluctuation. Content dependent fluctuation might be easily observable even at large but finite N unlike the observation of violation of $|N_{+1}(X, N)/N - 1/2| < \epsilon$. This is because former is only a relative property (i.e., we study fluctuation of one ensemble compared to that of another ensemble) unlike the latter. In the latter we have to wait for rare events to occur but it is not required in case of the former as we are interested only in the relative fluctuation which do not depend on rare events alone.

8.9.2 *A priori* probability may lead to information loss

If $\lim_{N \to \infty} N_{+1}(X, N)/N = 1/2$ always then *a priori* assumption of probability 1/2 becomes useless and pointless (because then we can take former itself as our starting point instead of assuming *a priori* probability 1/2). Because it is not so, *a priori* assumption of probability 1/2 makes sense and makes life easy, makes predictions and calculations mathematically neat and rigorous (Bayes rule, Borel sets etc.), and quantitatively precise. But it may lead to information loss as shown by FQM in chapter 5.

8.9.3 No pointwise convergence of limiting relative frequency follows directly from randomness: Experimental verification not necessary

The following statement is not correct: "Whether $\lim_{N\to\infty} N_{+1}(X, N)/N$ always converges pointwise to $1/2$ or not has to be found only experimentally." This is because as shown in Appendix 8.9, given the definition, meaning, and nature of random phenomena, one can show using the definition of pointwise convergence that $\lim_{N\to\infty} N_{+1}(X, N)/N$ cannot always converge pointwise to $1/2$. Hence experiment is sufficient but not necessary to arrive at this result. Moreover $N \to \infty$ number of trials of random variable cannot be realised in a real world experiment but only in a thought experiment i.e., at the conceptual level only. Obtaining always a given constant value $(1/2)$ out of every infinite set of random data contradicts the very meaning, definition, and nature of randomness [vL96].

8.9.4 Implications of no pointwise convergence

No pointwise convergence (Appendix 8.9) has following implications.

The fact that $\lim_{N\to\infty} N_{+1}(X^{\theta=\pi/2}, N)/N$ cannot always converge pointwise to $1/2$, opens up every other possibility including converging pointwise to a value different from $1/2$, even for the random variable $X^{\theta=\pi/2}$ (other possibility is oscillation of $\lim_{N\to\infty} N_{+1}(X^{\theta=\pi/2}, N)/N$ i.e., not converging pointwise to any fixed value). The two cases viz., $\theta = \pi/2$ and $\theta \neq \pi/2$ are distinguished by their fluctuation i.e., for $\theta = \pi/2$ we have

$$F(X^{\theta=\pi/2} = +1) = \cos^2(\theta/2)|_{\theta=\pi/2} + \kappa(X^{\theta=\pi/2} = +1)$$

whereas for $\theta \neq \pi/2$ we have

$$F(X^{\theta \neq \pi/2} = +1) = \cos^2(\theta/2)|_{\theta \neq \pi/2} + \kappa(X^{\theta \neq \pi/2} = +1).$$

Fluctuation of $\kappa(X^{\theta = \pi/2} = +1)$ is different from that of $\kappa(X^{\theta \neq \pi/2} = +1)$. Moreover $F(X^{\theta = \pi/2} = +1)$ fluctuates around $1/2$ whereas $F(X^{\theta \neq \pi/2} = +1)$ do not fluctuate around $1/2$. Note that $1/2$ in $F(X^{\theta = \pi/2} = +1)$ is just for the sake of convenience. We could have well chosen a value slightly different from $1/2$ as well i.e., we could have defined

$$F(X^{\theta} = +1) = (\cos^2(\theta/2) + \epsilon) + \kappa(X^{\theta} = +1)$$

where $|\epsilon| > 0$. (Note that as ϵ is a constant, it can be absorbed into $\kappa(...)$ term. ϵ is an overall shift of reference point common to all values of θ. Hence it is like change of coordinate system. Similar to the proof in Appendix 8.9, one can also show that $\lim_{N \to \infty} N_{+1}(X^{\theta}, N)/N$ cannot always converge pointwise to $1/2 + \epsilon$. For $\theta = 0, \pi$ we will have $\kappa(X^{0,\pi} = +1) = -\epsilon$.) This is because, due to no pointwise convergence (and hence fundamental uncertainty/fluctuation represented by $\kappa(...)$ term) we cannot strictly say that $F(X^{\theta = \pi/2} = +1)$ will fluctuate strictly and symmetrically around a value which is precisely $1/2$. There is no compelling reason to choose $1/2$. $1/2$ is motivated by symmetry and convenience. Even if we repeat infinitely many times the experiment involving $N \to \infty$ number of trials, still we will not come to know with certainty if $F(X^{\theta = \pi/2} = +1)$ fluctuates symmetrically around $1/2$ or not. This is due to fundamental uncertainty arising due to intrinsic randomness in measurement outcomes. What really matters and one can talk of is the relative fluctuation i.e., fluctuation of $F(X^{\theta = \pi/2} = +1)$ will be different compared to that of $F(X^{\theta \neq \pi/2} = +1)$. And the fluctuation of $F(X^{\theta} = +1)$ depends on θ (see Appendix 8.11 in this regard).

Moreover FQM predicts different fluctuations in two different ensemble preparation procedures even at large but finite N which is the case of practical interest. In this case there is no question of whether limit exists or not. We have considered the limit $N \to \infty$ for the sake of mathematical rigor and to show that even in the limit $N \to \infty$ (which can be realised at least in a thought experiment) fluctuation do not vanish unlike in KQM and hence there exists content dependent fluctuation. Physics is same at all N. And hence if content dependent fluctuation exists in the limit $N \to \infty$ then it should also be present even at large but finite N as well.

8.10   Anderson orthogonality catastrophe

In the limit $\mathcal{M} \to \infty$, due to Anderson's orthogonality catastrophe (AOC) [And67] we obtain $|\langle \psi_j^A | \psi_k^B \rangle| \to 0 \ \forall j, k$. However the states $|\psi_k^B\rangle$'s will be still linearly dependent on $|\psi_j^A\rangle$'s. This is a seemingly strange property exhibited only by infinite tensor product non-separable Hilbert spaces [vN76]. And hence within KQM, in spite of AOC, it is still not possible to distinguish between the two preparation procedures A and B [Che98]. Proof of this will be published elsewhere.

8.11   Justification of the assumption that $\kappa(X^\theta = +1)$ depends on θ

The fact that $F(X^\theta = +1)$ cannot always converge pointwise to $\cos^2(\theta/2)$ proves the existence of fluctuation term i.e., $\kappa(.)$, but it does not say if $\kappa(.)$ depends on θ or not. Hence in Eq. (5.4) we have implicitly assumed that $\kappa(.)$ will depend on θ. This can be justified as follows. KQM predicts that variance (which is a measure of fluctuation),

$\text{Var}(X^\theta) = \langle X^{\theta 2} \rangle - \langle X^\theta \rangle^2 = \sin^2 \theta$. This has been tested experimentally to a good extent. Hence from this we can deduce that fluctuation will be maximum for $\theta = \pi/2$ and fluctuation gradually decreases as θ either decreases to 0 or increases to π. Hence it is an experimental fact that fluctuation will depend on content/state i.e., θ. This justifies the assumption that fluctuation of $F(X^\theta = +1)$ (and hence $\kappa(X^\theta = +1)$) will depend on θ.

8.12 Physical meaning and significance of sample mean

Consider sample means $S(\text{A}, M)$, $S(\text{B}, M)$ as defined in Eqs. (5.5, 5.9) respectively. They are the average of final (i.e., after applying $R_x(X^\Theta)$) σ_z measurement (carried out by Bob) outcomes X_i^θ's. In procedure A, $X_i^\theta \in \{X_i^{\theta_1}, X_i^{\theta_2}, X_i^{\pi-\theta_1}, X_i^{\pi-\theta_2}\}$. Whereas in procedure B, $X_i^\theta \in \{X_i^{\pi/2}\}$ (because in procedure B, with respect to σ_z measurement outcomes, the states $|+\rangle$ and $|-\rangle$ are equivalent). For the sake of ease, let us consider $S(\text{B}, M)$ (because in procedure B, the set to which X_i^θ belongs to, has only one element). We have defined

$$S(\text{B}, M) = \frac{1}{M} \sum_{i=1}^{M} X_i^{\pi/2}.$$

$\Rightarrow S(\text{B}, M = 1) = X_1^{\pi/2}$. Hence we can rewrite

$$S(\text{B}, N) = \frac{1}{N}(N_{+1}(S(\text{B}, M = 1), N)$$

$$-N_{-1}(S(\text{B}, M = 1), N))$$

$$= \frac{1}{N}(2N_{+1}(S(\text{B}, M = 1), N) - N)$$

$$(\because N_{+1}(S(\text{B}, M = 1), N) + N_{-1}(S(\text{B}, M = 1), N) = N)$$

$$= 2F_N(S(\text{B}, M = 1) = +1) - 1 = 2F_N(X_1^{\pi/2} = +1) - 1.$$

Similarly one can obtain $S(\text{A}, N) = 2F_N(S(\text{A}, M = 1) = +1) - 1$. Sample means are used to study the relative fluctuation in the two procedures A and B.

8.13 Evaluating $\limsup_{N\to\infty} \frac{N_{+1}(X_1^{\pi-\theta_1}, N_0(X_1, N))}{N}$

If $\{a_N\}$ and $\{b_N\}$ are sequences of non-negative numbers, then

$$\liminf_{N\to\infty} a_N \liminf_{N\to\infty} b_N \le \liminf_{N\to\infty}(a_N b_N)$$

$$\le \liminf_{N\to\infty} a_N \limsup_{N\to\infty} b_N$$

$$\le \limsup_{N\to\infty}(a_N b_N) \le \limsup_{N\to\infty} a_N \limsup_{N\to\infty} b_N,$$

$$\text{and } \liminf_{N\to\infty} a_N + \liminf_{N\to\infty} b_N \le \liminf_{N\to\infty}(a_N + b_N)$$

$$\le \liminf_{N\to\infty} a_N + \limsup_{N\to\infty} b_N$$

$$\le \limsup_{N\to\infty}(a_N + b_N) \le \limsup_{N\to\infty} a_N + \limsup_{N\to\infty} b_N$$

$$(8.24)$$

[KN00, Roy68, Soh06]. Then using ineq. (8.24) we obtain,

$$\limsup_{N\to\infty} \frac{N_{+1}(X_1^{\pi-\theta_1}, N_0(X_1, N))}{N}$$
$$\leq (\sin^2\frac{\theta_1}{2} + \kappa(X_1^{\pi-\theta_1} = +1, 0(X_1)))(\frac{1}{2} + \kappa(X_1 = 0)).$$

8.14 Case where $\theta_1 = \theta_2 = 0, \pi/2$

For $\theta_1 = \theta_2 = 0$, $N_{+1}(X_1^{\theta_1=0}, N_{+1}(X_1, N)) = N_{+1}(X_1, N)$, and $N_{+1}(X_1^{\pi-\theta_1=\pi}, N_0(X_1, N)) = 0$.

$$\Rightarrow F(S(\mathrm{A}, M = 1) = +1) = \limsup_{N\to\infty} \frac{N_{+1}(S(\mathrm{A}, M = 1), N)}{N}$$
$$= \limsup_{N\to\infty} \frac{N_{+1}(X_1, N)}{N} = 1/2 + \kappa(X_1 = +1).$$

Alternatively, for $N < \infty$ with $\theta_1 = \theta_2 = 0$, we have $\kappa_N(X_1^{\theta_1=0} = +1, +1(X_1)) = 0, \kappa_N(X_1^{\pi-\theta_1=\pi} = +1, 0(X_1)) = 0$. Then from ineq. (5.8) we obtain $F_N(S(\mathrm{A}, M = 1) = +1) = 1/2 + \kappa_N(X_1 = +1)$. $\Rightarrow \limsup_{N\to\infty} F_N(S(\mathrm{A}, M = 1) = +1) = 1/2 + \kappa(X_1 = +1)$.

For $\theta_1 = \theta_2 = \pi/2$,

$$N_{+1}(S(\mathrm{A}, M = 1), N) = N_{+1}(X_1^{\theta_1=\pi/2}, N_{+1}(X_1, N))$$
$$+ N_{+1}(X_1^{\pi-\theta_1=\pi/2}, N_0(X_1, N))$$
$$= N_{+1}(X_1^{\pi/2}, N_{+1}(X_1, N) + N_0(X_1, N))$$
$$= N_{+1}(X_1^{\pi/2}, N). \qquad (8.25)$$

$$\Rightarrow F(S(\mathrm{A}, M = 1) = +1) = \limsup_{N \to \infty} \frac{N_{+1}(S(\mathrm{A}, M = 1), N)}{N}$$

$$= \limsup_{N \to \infty} \frac{N_{+1}(X_1^{\pi/2}, N)}{N}$$

$$= 1/2 + \kappa(X_1^{\pi/2} = +1) = 1/2 + \kappa(X_1 = +1).$$

8.15 limit infimum

If we define

$$F'(S(\mathrm{A}, M = 1) = +1) = \liminf_{N \to \infty} \frac{N_{+1}(S(\mathrm{A}, M = 1), N)}{N}$$

$$(8.26)$$

then using ineq. (8.24), we obtain for the case $\theta_1 = \theta_2$ in Eq. (5.3),

$$F'(S(\mathrm{A}, M = 1) = +1) \geq \frac{1}{2}$$

$$+\kappa'(X_1 = +1)\left(\cos^2(\theta_1/2) + \kappa'(X_1^{\theta_1} = +1, +1(X_1))\right)$$

$$+\kappa'(X_1 = 0)\left(\sin^2(\theta_1/2) + \kappa'(X_1^{\pi-\theta_1} = +1, 0(X_1))\right)$$

$$+\frac{1}{2}\left(\kappa'(X_1^{\theta_1} = +1, +1(X_1)) + \kappa'(X_1^{\pi-\theta_1} = +1, 0(X_1))\right)$$

where $\kappa'(\cdots)$'s correspond to limit infimum.

8.16 On the observability of content dependent fluctuation

The fact that limiting relative frequency cannot always converge pointwise to a given constant value (real number) proves the existence of fluctuation term $\kappa(.)$ and hence

content dependent fluctuation (i.e., fluctuation of $F(S(\mathrm{A}, M = 1) = +1)$ depends on θ_1, θ_2) (see Appendix 8.11). However it should be noted that observing content dependent fluctuation may not be as difficult as observing violation of the requirement for pointwise convergence e.g., observing the violation of $|N_{+1}(X_1, N)/N - 1/2| < \epsilon$ where $\epsilon > 0, N < \infty$, usually becomes difficult if we choose N sufficiently large (this is justified by the stabilization of relative frequency which is an experimental fact [Gut05]). This is because, former requires observing relative fluctuation only, which do not depend only on rare events unlike the latter which depends only on rare events.

8.17 Perfect anti-correlation of singlet in FQM

We can rewrite $\lim_{N \to \infty} S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, N)$, defined in Sec. 5.7 as follows:

$$\lim_{N \to \infty} S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, N) = \lim_{N \to \infty}$$
$$\frac{N_{+1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N) - N_{-1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N)}{N}.$$

We have

$$N_{+1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N)$$

$$= N_{+1+1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N)$$

$$+ N_{-1-1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N) = 0 + 0.$$

$$N_{-1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N)$$

$$= N_{+1-1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N)$$

$$+ N_{-1+1}(S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, M = 1), N)$$

$$= N_{+1}(\sigma_z^{\mathcal{A}}, N) + N_{-1}(\sigma_z^{\mathcal{A}}, N) = N.$$

$$\Rightarrow \lim_{N \to \infty} S(\sigma_z^{\mathcal{A}} \sigma_z^{\mathcal{B}}, N)$$

$$= -\lim_{N \to \infty} \frac{N_{+1}(\sigma_z^{\mathcal{A}}, N) + N_{-1}(\sigma_z^{\mathcal{A}}, N)}{N} = -1.$$

8.18 The case when $1 \ll N < \infty$

Consider the case when $1 \ll N < \infty$. Define

$$F_N(X = +1) = \frac{N_{+1}(X, N)}{N} := \frac{1}{2} + \kappa_N(X = +1) \tag{8.27}$$

where $\kappa_N(X = +1)$ is a random variable which takes values in $[-\epsilon_N, \delta_N]$ ($\epsilon_N > 0$, $\delta_N > 0$). Then the expression corresponding to ineq. (5.7) will be the following,

$$\frac{N_{+1}(X_1^{\theta_1}, N_{+1}(X_1, N))}{N_{+1}(X_1, N)} \frac{N_{+1}(X_1, N)}{N}$$
$$= (\cos^2(\theta_1/2) + \kappa_N(X_1^{\theta_1} = +1, +1(X_1)))$$
$$\times (1/2 + \kappa_N(X_1 = +1)), \tag{8.28}$$

for $N_{+1}(X_1, N) > 0$. This shows that, in all the results derived in the main text, we just have to replace $\kappa(\cdots)$'s with the corresponding $\kappa_N(\cdots)$'s, and inequalities become equalities. Of course the constraint that the terms in the denominators should be greater than zero should be satisfied (like $N_{+1}(X_1, N) > 0$ in Eq. (8.28)). Further note that $\limsup_{N \to \infty} F_N(X = +1) = F(X = +1)$ and hence $\limsup_{N \to \infty} \kappa_N(X = +1) = \kappa(X = +1)$ as required. Similarly we obtain $\limsup_{N \to \infty} \kappa_N(\cdots) = \kappa(\cdots)$.

Further note that when N is very small (say e.g., $1 \leq N \leq 10$), then both $F_N(S(\mathrm{A}, M = 1) = +1)$ and $F_N(S(\mathrm{B}, M = 1) = +1)$ will easily saturate i.e., will easily take maximum and minimum possible values which are 1 and 0 respectively. Hence Bob cannot distinguish. Fig. 5.1 is helpful in understanding this point.

135

8.19 Case where $\theta_2 \neq \theta_1$ in Eq. (5.3)

Let $M = 1$. Let $N_{x_1 x_1^\Theta}((X_1, X_1^\Theta), N)$ be the number of $X_1 = x_1$ and $X_1^\Theta = x_1^\Theta$ outcomes in N independent trials each of X_1 and X_1^Θ. Then we have the following identity $N_{x_1 x_1^\Theta}((X_1, X_1^\Theta), N) = N_{x_1}(X_1, N_{x_1^\Theta}(X_1^\Theta, N))$ ($\because$ events are independent) where $N_{x_1^\Theta}(X_1^\Theta, N)$ is the number of x_1^Θ outcomes in N independent trials of X_1^Θ, $x_1 = +1, 0; x_1^\Theta = \theta_1, \theta_2$; and $N_{\theta_1}(X_1^\Theta, N) + N_{\theta_2}(X_1^\Theta, N) = N$. Further we have

$$N_{+1}(S(\text{A}, M = 1), N) = N_{+1}(X_1^{\theta_1}, N_{+1\theta_1}((X_1, X_1^\Theta), N))$$

$$+ N_{+1}(X_1^{\theta_2}, N_{+1\theta_2}((X_1, X_1^\Theta), N))$$

$$+ N_{+1}(X_1^{\pi - \theta_1}, N_{0\theta_1}((X_1, X_1^\Theta), N))$$

$$+ N_{+1}(X_1^{\pi - \theta_2}, N_{0\theta_2}((X_1, X_1^\Theta), N))$$

where $N_{+1\theta_1}((X_1, X_1^\Theta), N) + N_{+1\theta_2}((X_1, X_1^\Theta), N) + N_{0\theta_1}((X_1, X_1^\Theta), N) + N_{0\theta_2}((X_1, X_1^\Theta), N) = N$. Then using ineq. (8.24) we obtain

$$\limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_1}, N_{+1\theta_1}((X_1, X_1^\Theta), N))}{N}$$

$$= \limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_1}, N_{+1\theta_1}((X_1, X_1^\Theta), N))}{N_{+1\theta_1}((X_1, X_1^\Theta), N)}$$

$$\times \frac{N_{+1\theta_1}((X_1, X_1^\Theta), N)}{N}$$

$$= \limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_1}, N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N)))}{N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N))}$$

$$\times \frac{N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N))}{N_{\theta_1}(X_1^\Theta, N)} \frac{N_{\theta_1}(X_1^\Theta, N)}{N}$$

$$\leq \limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_1}, N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N)))}{N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N))}$$

$$\times \limsup_{N \to \infty} \frac{N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N))}{N_{\theta_1}(X_1^\Theta, N)} \limsup_{N \to \infty} \frac{N_{\theta_1}(X_1^\Theta, N)}{N},$$

for $N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N \to \infty)) > 0, N_{\theta_1}(X_1^\Theta, N \to \infty) > 0$. Substituting $\theta_1 = 0, \theta_2 = \pi$ in the above expression, we obtain

$$\limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_1}, N_{+1\theta_1}((X_1, X_1^\Theta), N))}{N}$$
$$\leq (1/2 + \kappa(X_1 = +1, \theta_1(X_1^\Theta)))(1/2 + \kappa(X_1^\Theta = \theta_1))$$

$(\because N_{+1}(X_1^{\theta_1=0}, N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N))) = N_{+1}(X_1, N_{\theta_1}(X_1^\Theta, N)))$. Similarly we obtain

$$\limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_2}, N_{+1\theta_2}((X_1, X_1^\Theta), N))}{N}$$
$$\leq \limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_2}, N_{+1}(X_1, N_{\theta_2}(X_1^\Theta, N)))}{N_{+1}(X_1, N_{\theta_2}(X_1^\Theta, N))}$$
$$\times \limsup_{N \to \infty} \frac{N_{+1}(X_1, N_{\theta_2}(X_1^\Theta, N))}{N_{\theta_2}(X_1^\Theta, N)} \limsup_{N \to \infty} \frac{N_{\theta_2}(X_1^\Theta, N)}{N}.$$

Substituting $\theta_1 = 0, \theta_2 = \pi$ in the above expression, we obtain

$$\limsup_{N \to \infty} \frac{N_{+1}(X_1^{\theta_2}, N_{+1\theta_2}((X_1, X_1^\Theta), N))}{N} = 0$$

$(\because N_{+1}(X_1^{\theta_2=\pi}, N_{+1}(X_1, N_{\theta_2}(X_1^\Theta, N))) = 0)$. Similarly

$$\limsup_{N \to \infty} \frac{N_{+1}(X_1^{\pi-\theta_1}, N_{0\theta_1}((X_1, X_1^\Theta), N))}{N}$$
$$\leq \limsup_{N \to \infty} \frac{N_{+1}(X_1^{\pi-\theta_1}, N_0(X_1, N_{\theta_1}(X_1^\Theta, N)))}{N_0(X_1, N_{\theta_1}(X_1^\Theta, N))}$$
$$\times \limsup_{N \to \infty} \frac{N_0(X_1, N_{\theta_1}(X_1^\Theta, N))}{N_{\theta_1}(X_1^\Theta, N)} \limsup_{N \to \infty} \frac{N_{\theta_1}(X_1^\Theta, N)}{N}.$$

Substituting $\theta_1 = 0, \theta_2 = \pi$ in the above expression, we obtain

$$\limsup_{N \to \infty} \frac{N_{+1}(X_1^{\pi-\theta_1}, N_{0\theta_1}((X_1, X_1^\Theta), N))}{N} = 0$$

$(\because N_{+1}(X_1^{\pi-\theta_1=\pi}, N_0(X_1, N_{\theta_1}(X_1^\Theta, N))) = 0)$. Similarly

$$\limsup_{N\to\infty} \frac{N_{+1}(X_1^{\pi-\theta_2}, N_{0\theta_2}((X_1, X_1^\Theta), N))}{N}$$

$$\leq \limsup_{N\to\infty} \frac{N_{+1}(X_1^{\pi-\theta_2}, N_0(X_1, N_{\theta_2}(X_1^\Theta, N)))}{N_0(X_1, N_{\theta_2}(X_1^\Theta, N))}$$

$$\times \limsup_{N\to\infty} \frac{N_0(X_1, N_{\theta_2}(X_1^\Theta, N))}{N_{\theta_2}(X_1^\Theta, N)} \limsup_{N\to\infty} \frac{N_{\theta_2}(X_1^\Theta, N)}{N}.$$

Substituting $\theta_1 = 0, \theta_2 = \pi$ in the above expression, we obtain

$$\limsup_{N\to\infty} \frac{N_{+1}(X_1^{\pi-\theta_2}, N_{0\theta_2}((X_1, X_1^\Theta), N))}{N}$$

$$\leq (1/2 + \kappa(X_1 = 0, \theta_2(X_1^\Theta)))(1/2 + \kappa(X_1^\Theta = \theta_2))$$

$(\because N_{+1}(X_1^{\pi-\theta_2=0}, N_0(X_1, N_{\theta_2}(X_1^\Theta, N))) = N_0(X_1, N_{\theta_2}(X_1^\Theta, N)))$. Substituting the above expressions into Eq. (5.6), we obtain for the case $\theta_1 = 0, \theta_2 = \pi$, the following expression

$$F(S(\mathrm{A}, M = 1) = +1) \leq \frac{1}{2} + \frac{\kappa(X_1^\Theta = \theta_1) + \kappa(X_1^\Theta = \theta_2)}{2}$$

$$+ \big(\kappa(X_1 = +1, \theta_1(X_1^\Theta)) + \kappa(X_1 = 0, \theta_2(X_1^\Theta))\big)/2$$

$$+ \kappa(X_1^\Theta = \theta_1)\kappa(X_1 = +1, \theta_1(X_1^\Theta))$$

$$+ \kappa(X_1^\Theta = \theta_2)\kappa(X_1 = 0, \theta_2(X_1^\Theta)). \tag{8.29}$$

Further, we can rewrite,

$$\limsup_{N\to\infty} S(\text{A}, N) = \limsup_{N\to\infty}$$

$$\frac{N_{+1}(S(\text{A}, M=1), N) - (N - N_{+1}(S(\text{A}, M=1), N))}{N}$$

$$= 2F(S(\text{A}, M=1) = +1) - 1$$

$$= \kappa(X_1^\Theta = \theta_1) + \kappa(X_1^\Theta = \theta_2)$$

$$+\kappa(X_1 = +1, \theta_1(X_1^\Theta)) + \kappa(X_1 = 0, \theta_2(X_1^\Theta))$$

$$+2\kappa(X_1^\Theta = \theta_1)\kappa(X_1 = +1, \theta_1(X_1^\Theta))$$

$$+2\kappa(X_1^\Theta = \theta_2)\kappa(X_1 = 0, \theta_2(X_1^\Theta)) \tag{8.30}$$

where we used Eq. (5.6) and expression (8.29). Similarly we can rewrite,

$$\limsup_{N\to\infty} S(\text{B}, N) = \limsup_{N\to\infty}$$

$$\frac{N_{+1}(S(\text{B}, M=1), N) - (N - N_{+1}(S(\text{B}, M=1), N))}{N}$$

$$= 2\kappa(X_1 = +1) = 2\kappa(X_1^\Theta = \theta_1) \tag{8.31}$$

where we used Eq. (5.10).

8.20 Associating normal distribution with the fluctuation of $\kappa_N(...)$ terms for practical purposes

Here we quantify (for practical purposes) using KQM, the content dependent fluctuation in $S(\text{A}, N)$, and the fluctuation of $S(\text{B}, N)$.

8.20.1 $S(\mathrm{A}, N) \approx \kappa_{M_1}(X_1 = +1) + \kappa_{M_2}(X_1 = 0) + 4\kappa_N(X_1^{\Theta} = \theta_1)\kappa_N(X_1 = +1)$ **for** $N \gg 1, \theta_1 = 0, \theta_2 = \pi$

In the case $\theta_1 = 0, \theta_2 = \pi$ in Eq. (5.3), for $N \gg 1$, we can make following approximations:

$$\frac{N_{+1}(X_1, N_{\theta_1}(X_1^{\Theta}, N))}{N_{\theta_1}(X_1^{\Theta}, N)} = \frac{1}{2} + \kappa_N(X_1 = +1, \theta_1(X_1^{\Theta}))$$

$$\approx \frac{N_{+1}(X_1, M_1)}{M_1} = \frac{1}{2} + \kappa_{M_1}(X_1 = +1), \tag{8.32}$$

$$\frac{N_0(X_1, N_{\theta_2}(X_1^{\Theta}, N))}{N_{\theta_2}(X_1^{\Theta}, N)} = \frac{1}{2} + \kappa_N(X_1 = 0, \theta_2(X_1^{\Theta}))$$

$$\approx \frac{N_0(X_1, M_2)}{M_2} = \frac{1}{2} + \kappa_{M_2}(X_1 = 0) \tag{8.33}$$

where $M_1 = N/2, M_2 = N/2$ (for convenience we have assumed N to be even). It is important to note that M_1 number of trials of X_1 are independent and different from M_2 number of trials of X_1. This is represented by denoting each of the $N/2$ number of trials in Eqs. (8.32, 8.33) using different symbols i.e., M_1 and M_2. Further

$$\frac{N_{+1}(X_1, M_1)}{M_1} - \frac{N_0(X_1, M_2)}{M_2} = 2\frac{N_{+1}(X_1, N)}{N} - 1$$

$$\Rightarrow \kappa_{M_1}(X_1 = +1) - \kappa_{M_2}(X_1 = 0) = 2\kappa_N(X_1 = +1).$$

And $\kappa_N(X_1^{\Theta} = \theta_1) = -\kappa_N(X_1^{\Theta} = \theta_2)$. Substituting these into the finite N expression corresponding to expression (8.30), we obtain

$$S(\mathrm{A}, N) \approx \kappa_{M_1}(X_1 = +1) + \kappa_{M_2}(X_1 = 0)$$

$$+ 4\kappa_N(X_1^{\Theta} = \theta_1)\kappa_N(X_1 = +1). \tag{8.34}$$

8.20.2 Plotting the density of $F_N(S(A/B, M = 1) = +1)$

To experimentally study the fluctuation of $F_N(S(A/B, M = 1) = +1)$, we should repeat the experiment n times and plot the density of $F_N(S(A/B, M = 1) = +1)$ versus $F_N(S(A/B, M = 1) = +1)$ where density of $F_N(S(A/B, M = 1) = +1)$ is nothing but the ratio of number of times we get $F_N(S(A/B, M = 1) = +1) = y$ in n repetitions and $(n \times \delta F_N(S(A/B, M = 1) = +1))$ where $y \in [0, 1]$ and $\delta F_N(S(A/B, M = 1) = +1)(= 1/N)$ is the step size. For example, consider the simplest case of plotting the density of

$$F_N(S(B, M = 1) = +1)$$
$$= N_{+1}(S(B, M = 1), N)/N = N_{+1}(X_1^{\pi/2}, N)/N$$
$$= 1/2 + \kappa_N(X_1^{\pi/2} = +1). \tag{8.35}$$

$N_{+1}(X_1^{\pi/2}, N)$ takes value $y' \in \{0, 1, 2, ..., N\}$ and hence $F_N(S(B, M = 1) = +1)$ takes value $y \in \{0, 1/N, 2/N, ..., 1\}$. Hence $F_N(S(B, M = 1) = +1)$ tends to become a continuous random variable in the limit $N \to \infty$. Now we repeat n times the experiment involving N trials of $X_1^{\pi/2}$. Then we calculate the ratio of number of times we get $F_N(S(B, M = 1) = +1) = y$ in n repetitions and $(n \times (1/N))$. Then we plot this ratio versus y. For $N \gg 1$, we will obtain this plot to be approximately a Gaussian centered around $1/2$ (this we know from actual experiment) (KQM predicts that Gaussian will have mean $1/2$ and variance $1/(4N)$). This is how we can experimentally study the fluctuation of $F_N(S(B, M = 1) = +1)$, and hence the fluctuation of $\kappa_N(X_1^{\pi/2} = +1)$. Similarly, we can experimentally study the fluctuation of $F_N(S(A, M = 1) = +1)$. FQM predicts that the fluctuation of $F_N(S(A, M = 1) = +1)$ will be different from that of $F_N(S(B, M = 1) = +1)$.

Now we can safely (i.e., without loss of any fundamental content-dependent fluctuations) bring in KQM for practical purposes and quantify the fluctuation of $\kappa_N(...)$ terms

as follows. It is an experimental fact that if we plot the density of $F_N(X = +1)$ versus $F_N(X = +1)$, we obtain approximately a Gaussian function centered approximately around 1/2. Hence it is reasonable for practical purposes to associate a normal probability density function with the fluctuation of $\kappa_N(...)$ terms, i.e.,

$$f(\kappa_N(X_1 = x_1)) \approx \frac{1}{\sqrt{2\pi \mathrm{Var}(X_1)/N}} \exp(\frac{-\kappa_N(X_1 = x_1)^2}{2\mathrm{Var}(X_1)/N}),$$

(8.36)

where $f(Z)$ is the probability density function of the random variable Z, and $\mathrm{Var}(X_1) = \langle X_1^2 \rangle - \langle X_1 \rangle^2 = 1/4$ is the variance of X_1. Note that we can associate mean zero with every $\kappa(...)$ term. This is because, according to KQM,

$$\langle F_N(X = +1) \rangle = \langle X \rangle = 1/2 \Rightarrow \langle \kappa_N(X = +1) \rangle = 0,$$
$$\mathrm{Var}(F_N(X = +1)) = \frac{\mathrm{Var}(X)}{N} = \frac{1}{4N} = \mathrm{Var}(\kappa_N(X = +1)),$$
$$\langle F_N(X = +1) \rangle = \langle F_N(X^\Theta = \theta_1) \rangle,$$
$$\mathrm{Var}(F_N(X = +1)) = \mathrm{Var}(F_N(X^\Theta = \theta_1)).$$

(8.37)

Further, it is important to note that from a foundational perspective, fluctuation of $\kappa_N(X_1 = +1)$ do not vanish even in the limit $N \to \infty$, contrary to the approximation in (8.36), which becomes a "delta function". This is due to no pointwise convergence of LRF, always to 1/2. Note that for notational convenience, we are using the same symbol for the random variables $\kappa_N(...)$'s and also the values they take. Its meaning should be understood from the context of usage. To associate an approximate probability density

function with $4\kappa_N(X_1 = +1)\kappa_N(X_1^\Theta = \theta_1)$ in expression (8.34), we proceed as follows:

$$f(\zeta = 4\kappa_N(X_1 = +1)\kappa_N(X_1^\Theta = \theta_1))$$

$$\approx \int_{-\infty}^{\infty} d\kappa_N(X_1^\Theta = \theta_1) \, f(\zeta|\kappa_N(X_1^\Theta = \theta_1))f(\kappa_N(X_1^\Theta = \theta_1)),$$

(8.38)

where $f(\zeta, \kappa_N(X_1^\Theta = \theta_1)) = f(\zeta|\kappa_N(X_1^\Theta = \theta_1))f(\kappa_N(X_1^\Theta = \theta_1))$. Note that ζ depends on $\kappa_N(X_1^\Theta = \theta_1)$ and hence $f(\zeta|\kappa_N(X_1^\Theta = \theta_1)) \neq f(\zeta)$.

Theorem-1 [Ros10]: If X is a normally distributed random variable with mean μ and variance σ^2, then $Y = aX + b$ is also a normally distributed random variable with mean $a\mu + b$ and variance $a^2\sigma^2$ where a, b are constants.

Using approximations (8.36) and (8.38), and theorem-1, we obtain

$$f(\zeta = 4\kappa_N(X_1 = +1)\kappa_N(X_1^\Theta = \theta_1))$$

$$\approx \int_{-\infty}^{\infty} \frac{d\kappa_N(X_1^\Theta = \theta_1)}{\sqrt{2\pi\mathrm{Var}(X_1)/N}} \exp\left(\frac{-\kappa_N(X_1^\Theta = \theta_1)^2}{2\mathrm{Var}(X_1)/N}\right)$$

$$\times \sqrt{\frac{N}{32\pi\kappa_N(X_1^\Theta = \theta_1)^2\mathrm{Var}(X_1)}} \exp\left(\frac{-N\zeta^2}{32\kappa_N(X_1^\Theta = \theta_1)^2\mathrm{Var}(X_1)}\right), \quad (8.39)$$

where $\mathrm{Var}(X_1) = 1/4$, and where we have used the fact that $\kappa_N(X_1 = +1)$ and $\kappa_N(X_1^\Theta = \theta_1)$ are independent random variables and that the same variance $(= 1/(4N))$ must be associated with each of them (because X_1 and X_1^Θ differ only in the value assigned to their outcomes. See Eqs. (8.37) in this regard). If $\kappa_N(X_1 = +1)$ and $\kappa_N(X_1^\Theta = \theta_1)$ were not independent, then for a given value of $\kappa_N(X_1^\Theta = \theta_1)$, the probability distribution which we can associate with $\kappa_N(X_1 = +1)$ will depend on the given value of $\kappa_N(X_1^\Theta = \theta_1)$ as well. There is no analytical solution to the integral (8.39) (see [SMO12] in this regard, and for further details regarding approximate and numerical solutions to the integral), and in particular the distribution is not normal. Further

$\eta = \kappa_{M_1}(X_1 = +1) + \kappa_{M_2}(X_1 = 0)$ is normally distributed with mean 0 and variance $1/N$ [Ros10]. And η, ζ are not independent. Hence $S(A, N)$ cannot be normally distributed. We also have $S(B, N) = 2\kappa_N(X_1 = +1)$ (Eq. (8.31)). But

$$f(2\kappa_N(X_1 = +1))$$
$$\approx \frac{1}{\sqrt{8\pi \mathrm{Var}(X_1)/N}} \exp(\frac{-\kappa_N(X_1 = +1)^2}{8\mathrm{Var}(X_1)/N}). \tag{8.40}$$

Hence the fluctuations of sample means around 0 are different in the two preparation procedures A and B.

Bibliography

[AAP11]   S. Massar A. Acin and S. Pironio. Randomness vs non locality and entanglement. *arXiv*, 1107.2754v1 [quant-ph], 2011. 87, 112

[AB59]   Y. Aharonov and D. Bohm. Significance of electromagnetic potentials in the quantum theory. *Phys. Rev.*, 115:485–491, Aug 1959. 107

[ABD⁺10]   A Avella, G Brida, I P Degiovanni, M Genovese, M Gramegna, and P Traina. Experimental quantum-cryptography scheme based on orthogonal states. *Phys. Rev. A*, 82:062309, Dec 2010. 87

[AC17]   Anna Ananova and Rama Cont. Pathwise integration with respect to paths of finite quadratic variation. *Journal de Mathematiques Pures et Appliquees*, 107(6):737 – 757, 2017. 72, 82

[ACR16]   Yakir Aharonov, Eliahu Cohen, and Daniel Rohrlich. Nonlocality of the aharonov-bohm effect. *Phys. Rev. A*, 93:042110, Apr 2016. 107

[AK04]   Y. Aharonov and T. Kaufherr. The effect of a magnetic flux line in quantum theory. *Phys. Rev. Lett.*, 92:070404, Feb 2004. 107

[AL98]   Daniel S. Abrams and Seth Lloyd. Nonlinear quantum mechanics implies polynomial-time solution for np-complete and number p problems. *Phys. Rev. Lett.*, 81:3992–3995, Nov 1998. 107

[AMHR13]   Awad H. Al-Mohy, Nicholas J. Higham, and Samuel D. Relton. Computing the frechet derivative of the matrix logarithm and estimating the condition

number. *SIAM Journal on Scientific Computing*, 35(4):C394–C410, 2013. 57

[And67] P. W. Anderson. Infrared catastrophe in fermi gases with local scattering potentials. *Phys. Rev. Lett.*, 18:1049–1051, Jun 1967. 129

[AP58] A. Abragam and W. G. Proctor. Spin temperature. *Phys. Rev.*, 109:1441–1458, Mar 1958. 10

[Apo85] Tom M Apostol. *Mathematical Analysis*. Narosa publishing house, Second edition (1985). 74

[ARM11] Vikram Athalye, Soumya Singha Roy, and T. S. Mahesh. Investigation of the leggett-garg inequality for precessing nuclear spins. *Phys. Rev. Lett.*, 107:130402, Sep 2011. 34

[AUČ+05] A.Sen(De), U.Sen, Č.Brukner, V.Bužek, and M.Żukowski. *Phys. Rev. A*, 72:042310, 2005. 76

[Aud07] Jürgen Audretsch. *Entangled Systems: New Directions in Quantum Physics*. Wiley, 2007. 4, 5, 6, 7, 24, 116

[AW01] George B Arfken and Hans J Weber. *Mathematical methods for physicists*. Academic Press Elsvier, 2001. 3

[BAM16] Gaurav Bhole, V. S. Anjusha, and T. S. Mahesh. Steering quantum dynamics via bang-bang control: Implementing optimal fixed-point quantum search algorithm. *Phys. Rev. A*, 93:042339, Apr 2016. 15, 45

[BB84] C H Bennett and G Brassard. Quantum cryptography: Public key distribution and coin tossing. *International conference on computers, systems and signal processing Bangalore, India*, 1:175–179, Dec 1984. 80, 87

146

[BBA08] N. Boulant, D. Le Bihan, and A. Amadon. Strongly modulating pulses for counteracting rf inhomogeneity at high fields. *Magnetic Resonance in Medicine*, 60(3):701–708, 2008. 15

[BBB⁺06] E Biham, M Boyer, P O Boykin, T Mor, and V Roychowdhury. A proof of the security of quantum key distribution. *Jour. of Crypt.*, 19(4):381–439, Oct 2006. 87

[BBC⁺93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993. 80

[BBM92] C H Bennett, G Brassard, and N D Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992. 87

[BCJ⁺99] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for nmr quantum computing. *Phys. Rev. Lett.*, 83:1054–1057, Aug 1999. 64

[BCK12] J Barrett, R Colbeck, and A Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Phys. Rev. A*, 86:062326, Dec 2012. 87

[BcvH96] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A*, 54:1844–1852, Sep 1996. 80

[BE14] Costantino Budroni and Clive Emary. Temporal quantum correlations and leggett-garg inequalities in multilevel systems. *Phys. Rev. Lett.*, 113:050401, Jul 2014. 33, 42, 91

147

[Bel64] J S Bell. On the einstein podolsky rosen paradox. *Physics*, 1:195–200, 1964. 86

[Bel89] J S Bell. *Speakable and Unspeakable in Quantum Mechanics*. Cambridge university press, 1989. 84, 86

[Ben92] C H Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992. 87

[BF02] K Boström and T Felbinger. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.*, 89:187902, Oct 2002. 87

[BHD16] Yakov Ben-Haim and Maria Demertzis. Decision making in times of knightian uncertainty: An info-gap perspective. *Economics: The Open-Access, Open-Assessment E-Journal*, 10 (2016-23):1–29, 2016. 74

[BHW09] Todd A. Brun, Jim Harrington, and Mark M. Wilde. Localized closed timelike curves can perfectly distinguish quantum states. *Phys. Rev. Lett.*, 102:210402, May 2009. 80, 82, 103

[Bil95] P. Billingsley. *Probability and Measure*. Wiley, 1995. 72, 74, 105

[bJDBDJ05] Edited by John D. Barrow, Paul C. W. Davies, and Charles L. Harper Jr. *Science and Ultimate Reality-Quantum Theory, Cosmology and Complexity*. Cambridge University press, 2005. 1, 71

[BKH+16] A Boaron, B Korzh, R Houlmann, G Boso, C C W Lim, A Martin, and H Zbinden. Detector-device-independent quantum key distribution: Security analysis and fast implementation. *Jour. of App. Phy.*, 120(6):063101, 2016. 87

[BKW05] D.A. Belsley, E. Kuh, and R.E. Welsch. *Regression Diagnostics: Identifying Influential Data and Sources of Collinearity.* Wiley Series in Probability and Statistics. Wiley, 2005. 57

[Blo46] F. Bloch. Nuclear induction. *Phys. Rev.*, 70:460–474, Oct 1946. 12, 106

[BLSS09] Charles H. Bennett, Debbie Leung, Graeme Smith, and John A. Smolin. Can closed timelike curves or nonlinear quantum mechanics improve quantum state discrimination or help solve hard problems? *Phys. Rev. Lett.*, 103:170502, Oct 2009. 82

[Bra11] C Branciard. Detection loophole in bell experiments: How postselection modifies the requirements to observe nonlocality. *Phys. Rev. A*, 83:032123, Mar 2011. 101

[Cab02] A Cabello. Violating bell's inequality beyond cirel'son's bound. *Phys. Rev. Lett.*, 88:060403, Jan 2002. 86

[Cab08] Adán Cabello. Experimentally testable state-independent quantum contextuality. *Phys. Rev. Lett.*, 101:210401, Nov 2008. 29

[Cav96] John Cavanagh. *Protein NMR spectroscopy: principles and practice.* Academic Pr, 1996. 12, 26, 43, 44, 56

[Cav18] Eric G. Cavalcanti. Classical causal models for bell and kochen-specker inequality violations require fine-tuning. *Phys. Rev. X*, 8:021018, Apr 2018. 20, 90, 94

[CEB$^+$05] P. Cappellaro, J. Emerson, N. Boulant, C. Ramanathan, S. Lloyd, and D. G. Cory. Entanglement assisted metrology. *Phys. Rev. Lett.*, 94:020502, Jan 2005. 50

[CFH97] David G. Cory, Amr F. Fahmy, and Timothy F. Havel. Ensemble quantum computing by nmr spectroscopy. *Proceedings of the National Academy of Sciences*, 94(5):1634–1639, 1997. 16, 21, 28, 50

[CFS73] V. Capasso, D. Fortunato, and F. Selleri. Sensitive observables of quantum mechanics. *International Journal of Theoretical Physics*, 7(5):319–326, 1973. 24

[CGKL98] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung. Bulk quantum computation with nuclear magnetic resonance: theory and experiment. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 454(1969):447–467, 1998. 45

[Che98] Anthony Chefles. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A*, 239(6):339 – 347, 1998. 80, 129

[CHSH69] J F Clauser, M A Horne, A Shimony, and R A Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. 86

[Cir80] B S Cirel'son. Quantum generalizations of bell's inequality. *Lett. in Math. Phy.*, 4(2):93–100, 1980. 87, 94

[CLK+00] D.G. Cory, R. Laflamme, E. Knill, L. Viola, T.F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemariam, Y.S. Weinstein, and W.H. Zurek. Nmr based quantum information processing: Achievements and prospects. *Fortschritte der Physik*, 48(9-11):875–907, 2000. 50

[CM10] E. G. Cavalcanti and N. C. Menicucci. *arXiv:1004.1219 [quant-ph]*, 2010. 84

[CPH98]   D. G. Cory, M. D. Price, and T. F. Havel. *Physica D*, 120:82, 1998. 44, 50

[Cra53]   Harald Cramer. Richard von mises' work in probability and statistics. *The Annals of Mathematical Statistics*, 24(4):657–662, 1953. 72

[CTDL05] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum Mechanics.* John Wiley and Sons, 2005. xvi, 4, 6, 13, 22, 26, 72, 73, 104

[CZY+16] W J Chu, X L Zong, M Yang, G Z Pan, and Z L Cao. Optical simulation of a popescu-rohrlich box. *Scientific Reports*, 6:28351, Jun 2016. 101

[DDA16]   Shruti Dogra, Kavita Dorai, and Arvind. Experimental demonstration of quantum contextuality on an nmr qutrit. *Physics Letters A*, 380(22):1941 – 1946, 2016. 20, 25

[DiV]   David P DiVincenzo. The physical implementation of quantum computation. *arXiv*, quant-ph/0002077. 50

[DUF16]   I Derkach, V C Usenko, and R Filip. Preventing side-channel effects in continuous-variable quantum key distribution. *Phys. Rev. A*, 93:032309, Mar 2016. 87

[EBW04]   Richard R. Ernst, G. Bodenhausen, and A. Wokaun. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions.* Oxford Science Publications, 2004. 68

[Eke91]   Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. 21, 87, 98

[EMT11]   Reuven Eitan, Michael Mundt, and David J. Tannor. Optimal control

with accelerated convergence: Combining the krotov and quasi-newton methods. *Phys. Rev. A*, 83:053426, May 2011. 15

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935. 19, 90

[Fei67] G. Feinberg. Possibility of faster-than-light particles. *Phys. Rev.*, 159:1089–1105, Jul 1967. 107

[FHLD15] Guillaume Ferrand, Gaspard Huber, Michel Luong, and Herve Desvaux. Nuclear spin noise in nmr revisited. *The Journal of Chemical Physics*, 143(9):094201, 2015. 12, 106

[FPB⁺02] Evan M. Fortunato, Marco A. Pravia, Nicolas Boulant, Grum Teklemariam, Timothy F. Havel, and David G. Cory. Design of strongly modulating pulses to implement precise effective hamiltonians for quantum information processing. *The Journal of Chemical Physics*, 116(17):7599–7606, 2002. 15, 47, 53

[FRB18] Markus Frembs, Sam Roberts, and Stephen D Bartlett. Contextuality as a resource for measurement-based quantum computation beyond qubits. *New Journal of Physics*, 20(10):103011, oct 2018. 21

[Fri99] B Roy Frieden. *Physics from Fisher Information*. Cambridge University press, 1999. 7, 49, 67

[Fun01] B. M. Fung. Use of pairs of pseudopure states for nmr quantum computing. *Phys. Rev. A*, 63:022304, Jan 2001. 17, 44

[GA15] R Gallego and L Aolita. Resource theory of steering. *Phys. Rev. X*, 5:041008, Oct 2015. 94

[GBNP01] M Genovese, G Brida, C Novero, and E Predazziy. First experimental test of bell inequalities performed using a non-maximally entangled state. *Pram. jour. of phys.*, 56:153–159, Mar 2001. 89

[GG02] F Grosshans and P Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002. 87

[GHH+14] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, P. Joshi, W. Kłobus, and A. Wójcik. Quantifying contextuality. *Phys. Rev. Lett.*, 112:120401, Mar 2014. 20, 90, 94

[GKC+10] Otfried Gühne, Matthias Kleinmann, Adán Cabello, Jan-Åke Larsson, Gerhard Kirchmair, Florian Zähringer, Rene Gerritsma, and Christian F. Roos. Compatibility and noncontextuality for sequential measurements. *Phys. Rev. A*, 81:022121, Feb 2010. 24

[GLLL+11] I Gerhardt, Q Liu, A Lamas-Linares, J Skaar, V Scarani, V Makarov, and C Kurtsiefer. Experimentally faking the violation of bell's inequalities. *Phys. Rev. Lett.*, 107:170404, Oct 2011. 101

[GLTZ19] Sheldon Goldstein, Joel L. Lebowitz, Roderich Tumulka, and Nino Zanghi. Gibbs and boltzmann entropy in classical and quantum mechanics. *arXiv:1903.11870v1 [cond-mat.stat-mech]*, Mar 2019. 4, 5, 82, 83, 104, 106, 111, 113

[Gri95] David Jeffrey Griffiths. *Introduction to Quantum Mechanics*. Prentice Hall, 1995. 5, 72, 74

[GRTZ02] N Gisin, G Ribordy, W Tittel, and H Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002. 87

[Gup16] A. Gupta. *Introduction To Mathematical Analysis*. Academic Publishers, 2016. 74

[Gut05] Allan Gut. *Probability: A Graduate Course*. Springer, 2005. 5, 72, 74, 104, 110, 113, 115, 124, 126, 134

[GV95] L Goldenberg and L Vaidman. Quantum cryptography based on orthogonal states. *Phys. Rev. Lett.*, 75:1239–1243, Aug 1995. 87

[Haj12] Alan Hajek. Interpretations of probability. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2012 edition, 2012. 72

[HBD+15] B Hensen, H Bernien, A E Dreau, A Reiserer, N Kalb, M S Blok, J Ruitenberg, R F L Vermeulen, R N Schouten, C Abellan, W Amaya, V Pruneri, M W Mitchell, M Markham, D J Twitchen, D Elkouss, S Wehner, T H Taminiau, and R Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, October 2015. 89

[Hil00] M Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, Jan 2000. 87

[HMM16] Zixin Huang, Chiara Macchiavello, and Lorenzo Maccone. Usefulness of entanglement-assisted quantum metrology. *Phys. Rev. A*, 94:012101, Jul 2016. 65

[Hob11] David Hobson. *The Skorokhod Embedding Problem and Model-Independent Bounds for Option Prices*, pages 267–318. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011. 72, 74, 82

[Hom97]   Dipankar Home. *Conceptual Foundations of Quantum Physics: An Overview from Modern Perspectives.* Springer Science and Business media, 1997. 2, 4, 20, 21, 24, 33

[HPS$^+$06]   F. Hulpke, U. V. Poulsen, A. Sanpera, A. Sen(De), U. Sen, and M. Lewenstein. *Found. Phys.*, 36:477, 2006. 83

[HPS17]   A S Hejamadi, A Pathak, and R Srikanth. Quantum cryptography: Key distribution and beyond. *Quanta*, 6(1):1–47, 2017. 87

[HSM12]   G. C. Hegerfeldt and R. Sala Mayato. Discriminating between the von neumann and lüders reduction rule. *Phys. Rev. A*, 85:032116, Mar 2012. 33, 34, 42, 48

[Hua87]   K. Huang. *Statistical Mechanics.* John Wiley and Sons, 1987. 83

[IH05]   K Inoue and T Honjo. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Phys. Rev. A*, 71:042305, Apr 2005. 87

[JSK$^+$14]   Sharad Joshi, Abhishek Shukla, Hemant Katiyar, Anirban Hazra, and T. S. Mahesh. Estimating franck-condon factors using an nmr quantum processor. *Phys. Rev. A*, 90:022303, Aug 2014. 25

[JSW$^+$00]   T Jennewein, C Simon, G Weihs, H Weinfurter, and A Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84:4729–4732, May 2000. xix, 87, 96, 97, 101

[Kac56]   M. Kac. *in* Foundations of kinetic theory*, pp 171-197, J. Neyman (editor), Proceedings of the Third Berkeley Symposium on Mathematical Statistics and Probability, vol. III.* Berkeley: University of California Press, 1956. 83

[Kak00] S Kak. Quantum key distribution using three basis states. *Pram. jour. of phy.*, 54:709–713, May 2000. 87

[Kar95] Rajeeva L. Karandikar. On pathwise stochastic integration. *Stochastic Processes and their Applications*, 57(1):11 – 18, 1995. 72, 82

[KB13] Johannes Kofler and Časlav Brukner. Condition for macroscopic realism beyond the leggett-garg inequalities. *Phys. Rev. A*, 87:052115, May 2013. 72

[KCD] Sergey Knysh, Edward. H. Chen, and Gabriel. A. Durkin. True limits to precision via unique quantum probe. *arXiv*, 1402.0495. 50

[KDD13] Jan Kolodynski and Rafal Demkowicz-Dobrzanski. Efficient tools for quantum metrology with uncorrelated noise. *New Journal of Physics*, 15(7):073043, 2013. 51, 60, 61, 63

[KKM16] Hemant Katiyar, C. S. Sudheer Kumar, and T. S. Mahesh. Nmr investigation of contextuality in a quantum harmonic oscillator via pseudospin mapping. *Euro Physics Letters*, 113(2):20003, 2016. viii, 18, 34

[KLKW18] Sunho Kim, Longsuo Li, Asutosh Kumar, and Junde Wu. Characterizing nonclassical correlations via local quantum fisher information. *Phys. Rev. A*, 97:032326, Mar 2018. 7, 64, 108

[KM17] Deepak Khurana and T.S. Mahesh. Bang-bang optimal control of large spin systems: Enhancement of 13c-13c singlet-order at natural abundance. *Journal of Magnetic Resonance*, 284(Supplement C):8 – 14, 2017. 51

[KN00] W.J. Kaczor and M.T. Nowak. *Problems in Mathematical Analysis*. Number v. 1; v. 3 in Problems in Mathematical Analysis. American Mathematical Society, 2000. 78, 132

[Kni21] F. H. Knight. *Risk, Uncertainty, and Profit.* Houghton Mifflin Company, Boston, 1921. 74

[Kra16] W O Krawec. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quant. Info. Proc.*, 15(5):2067–2090, May 2016. 87

[KRMP12] Hemant Katiyar, Soumya Singha Roy, T. S. Mahesh, and Apoorva Patel. Evolution of quantum discord and its stability in two-qubit nmr systems. *Phys. Rev. A*, 86:012309, Jul 2012. 64

[KS67] S. Kochen and E. P. Specker. *J. Math. Mech.*, 17:59, 1967. 19, 20, 25, 90, 94

[KSM16] C.S. Sudheer Kumar, Abhishek Shukla, and T.S. Mahesh. Discriminating between luders and von neumann measuring devices: An nmr investigation. *Physics Letters A*, 380(43):3612 – 3616, 2016. viii, 32

[KSS+12] Xi Kong, Mingjun Shi, Fazhan Shi, Pengfei Wang, Pu Huang, Qi Zhang, Chenyong Ju, Changkui Duan, Sixia Yu, and Jiangfeng Du arXiv:1210.0961 [quant ph]. An experimental test of the non-classicality of quantum mechanics using an unmovable and indivisible system. *arXiv:1210.0961v1 [quant-ph]*, Oct 2012. 20, 25

[Kt05] Navin Khaneja *et. al.* Optimal control of coupled spin dynamics: design of nmr pulse sequences by gradient ascent algorithms. *Journal of Magnetic Resonance*, 172(2):296, 2005. 15, 28

[LÖ6] G. Lüders. Concerning the state-change due to the measurement process. *Annalen der Physik*, 15(9):663–670, 2006. 32, 33, 42, 91

[Lal04] F. Laloë. Do we really understand quantum mechanics? strange correlations, paradoxes and theorems. *arXiv*, 0209123v2 [quant-ph], Nov 2004. 2

[LC99] H K Lo and H F Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999. 87

[Lev08] Malcolm H Levitt. *Spin Dynamics-Basics of NMR*. John Wiley and Sons, Ltd, 2008. 9, 11, 12, 13, 14, 26, 44, 53, 55, 56, 58, 67

[LHFL14] Yi-Chan Lee, Min-Hsiu Hsieh, Steven T. Flammia, and Ray-Kuang Lee. Local pt symmetry violates the no-signaling principle. *Phys. Rev. Lett.*, 112:130404–1–130404–4, Apr 2014. 82, 106, 107

[LJL⁺10] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien. Quantum computers. *Nature*, 464:45–53, 2010. 50

[LM05] M Lucamarini and S Mancini. Secure deterministic communication without entanglement. *Phys. Rev. Lett.*, 94:140501, Apr 2005. 87

[LMXW11] Xiao-Ming Lu, Jian Ma, Zhengjun Xi, and Xiaoguang Wang. Optimal measurements to access classical correlations of two-qubit states. *Phys. Rev. A*, 83:012327, Jan 2011. 64

[LSV02] Stefano Liberati, Sebastiano Sonego, and Matt Visser. Faster-than-c signals, special relativity, and causality. *Annals of Physics*, 298(1):167 – 185, 2002. 107

[Lüd51] Gerhart Lüders. Über die zustandsänderung durch den meßprozeß. *Annalen der Physik*, 443(5-8):322–328, 1951. 33

[LZJ+06] Gui Lu Long, Yi-Fan Zhou, Jia-Qi Jin, Yang Sun, and Hai-Woong Lee; quant ph/0408079v3. Density matrix in quantum mechanics and distinctness of ensembles having the same compressed density matrix. *Foundations of Physics*, 36(8):1217–1243, 2006. 5, 6, 64, 76, 84, 104, 106

[May01] D Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, May 2001. 87

[MBC+12] Kavan Modi, Aharon Brodutch, Hugo Cable, Tomasz Paterek, and Vlatko Vedral. The classical-quantum boundary for correlations: Discord and related measures. *Rev. Mod. Phys.*, 84:1655–1707, Nov 2012. 64

[MDB+08] Thorsten Maly, Galia T. Debelouchina, Vikram S. Bajaj, Kan-Nian Hu, Chan-Gyu Joo, Melody L. Mak-Jurkauskas, Jagadishwar R. Sirigiri, Patrick C. A. van der Wel, Judith Herzfeld, Richard J. Temkin, and Robert G. Griffin. Dynamic nuclear polarization at high magnetic fields. *The Journal of Chemical Physics*, 128(5):052211, 2008. 50

[Mer85] N. David Mermin. Is the moon there when nobody looks? reality and the quantum theory. *Physics Today*, 38:38, 1985. 18

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, Dec 1990. 19, 90

[Mer93] N. D. Mermin. *Rev. Mod. Phys.*, 65:803, 1993.

[MKR+21] T S Mahesh, Deepak Khurana, Krithika V R, Sreejith G J, and C S Sudheer Kumar. Star-topology registers: Nmr and quantum information perspectives. *arXiv:2102.05203 [quant-ph]*, 2021. ix

[MMK08] Avik Mitra, T. S. Mahesh, and Anil Kumar. Nmr implementation of

adiabatic sat algorithm using strongly modulated pulses. *The Journal of Chemical Physics*, 128(12):124110–6, 2008. 15, 26

[MPA11]   L Masanes, S Pironio, and A Acin. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Comm.*, 2:238, Mar 2011. 87

[MRCL10] Osama Moussa, Colm A. Ryan, David G. Cory, and Raymond Laflamme. Testing contextuality on quantum ensembles with one clean qubit. *Phys. Rev. Lett.*, 104:160501, Apr 2010. xvi, 25, 26, 28, 31, 34, 102

[MSH+15] T. S. Mahesh, Abhishek Shukla, Swathi S. Hegde, C. S. Sudheer Kumar, Hemant Katiyar, Sharad Joshi, and K. R. Koteswara Rao. Ancilla assisted measurements on quantum ensembles: General protocols and applications in nmr quantum information processing. *Current Science*, 109:1987, 2015. ix

[MSKB17] T. S. Mahesh, C. S. Sudheer Kumar, and Udaysinh T. Bhosale. *Quantum Correlations in NMR Systems*, pages 499–516. Springer International Publishing, Cham, 2017. ix, 7

[Mun07]   James R Munkres. *Topology*. Pearson education Inc., Prentice hall, Second edition (2007). 74

[MV10]   P. M. Mathews and K. Venkatesan. *A Textbook of Quantum Mechanics*. Tata McGraw Hill Education, 2010. 72

[NC10]   Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010. 3, 4, 8, 16, 19, 21, 42, 50, 53, 73, 80, 86, 87, 88, 89, 94, 95

[Noh09] T G Noh. Counterfactual quantum cryptography. *Phys. Rev. Lett.*, 103:230501, Dec 2009. 87

[NTKK11] Makoto Negoro, Kenichiro Tateishi, Akinori Kagawa, and Masahiro Kitagawa. Scalable spin amplification with a gain over a hundred. *Phys. Rev. Lett.*, 107:050503, Jul 2011. 50

[OP09] C Osácar and A F Pacheco. Symmetry and degeneracy in quantum mechanics. self-duality in finite spin systems. *European Journal of Physics*, 30(4):891–899, jun 2009. 10

[Pal12] C. Palazuelos. *Phys. Rev. Lett.*, 109:190401, 2012. 76

[Paw10] M Pawłowski. Security proof for cryptographic protocols based only on the monogamy of bell's inequality violations. *Phys. Rev. A*, 82:032313, Sep 2010. 4, 82, 87, 98, 103

[PBKM17] Varad R. Pande, Gaurav Bhole, Deepak Khurana, and T. S. Mahesh. Strong algorithmic cooling in large star-topology quantum registers. *Phys. Rev. A*, 96:012330, Jul 2017. 51

[Pen06] Roger Penrose. *The Emperor's New Mind*. Oxford university press, 2006. 2, 3, 105

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3,4):107 – 108, 1990. 2, 19

[Per91] A Peres. Two simple proofs of the kochen-specker theorem. *Journal of Physics A: Mathematical and General*, 24(4):L175, 1991. 19, 90, 94

[Per95] Asher Peres. *Quantum Theory:Concepts and Methods*. Kluwer Academic Publishers, 1995. 7, 19

[Per96] A. Peres. *Phys. Rev. A*, 54:2685, 1996. 76

[Per02] Asher Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, 2002. 72

[PMA+19] S Pal, S Moitra, V S Anjusha, Anil Kumar, and T S Mahesh. Hybrid scheme for factorisation: Factoring 551 using a 3-qubit nmr quantum adiabatic processor. *Pram. jour. of phy.*, 92:1–8, Jan 2019. 4, 88

[PNMS18] Soham Pal, Naveen Nishad, T. S. Mahesh, and G. J. Sreejith. Temporal order in periodically driven spins in star-shaped clusters. *Phys. Rev. Lett.*, 120:180602, May 2018. 51

[Pop14] Sandu Popescu. Nonlocality beyond quantum mechanics. *Nat. Phys*, 10(4):264–270, 2014. 1, 2, 82

[Pop18] Sandu Popescu. Quantum states and knowledge: Between pure states and density matrices. *arXiv:1811.05472v1 [quant-ph]*, Nov 2018. 5, 76, 84, 104, 113

[PR94] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994. 72, 82, 85, 86

[PSCWH00] Roger Penrose, Abnor Shimony, Nancy Cart Wright, and Stephan Hawking. *The large, the small and the human mind.* Cambridge University press, Canto edition (2000). 5, 84, 104

[PSS+11] E Pomarico, B Sanguinetti, P Sekatski, H Zbinden, and N Gisin. Experimental amplification of an entangled photon: what if the detection loophole is ignored? *New Journal of Physics*, 13(6):063031, jun 2011. 101

[PT04] Asher Peres and Daniel R. Terno. Quantum information and relativity theory. *Rev. Mod. Phys.*, 76:93–123, Jan 2004. 72

[PZF⁺01] Xinhua Peng, Xiwen Zhu, Ximing Fang, Mang Feng, Kelin Gao, Xiaodong Yang, and Maili Liu. Preparation of pseudo-pure states by line-selective pulses in nuclear magnetic resonance. *Chemical Physics Letters*, 340(5):509 – 516, 2001. 16

[QVC⁺15] M T Quintino, T Vértesi, D Cavalcanti, R Augusiak, M Demianowicz, A Acín, and N Brunner. Inequivalence of entanglement, steering, and bell nonlocality for general measurements. *Phys. Rev. A*, 92:032107, Sep 2015. 94

[Raa18] Panu Raatikainen. Goedel's incompleteness theorems. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, fall 2018 edition, 2018. 105

[Ral99] T C Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999. 87

[Ral00] T C Ralph. Security of continuous-variable quantum cryptography. *Phys. Rev. A*, 62:062306, Nov 2000. 87

[Rei85] Federick Reif. *Fundamentals of statistical and thermal physics*. McGraw Hill book company, 1985. 9, 10

[Rei00] M D Reid. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. *Phys. Rev. A*, 62:062308, Nov 2000. 87

[Rig16] Candia Riga. A pathwise approach to continuous-time trading. *arXiv*, 1602.04946v1 [q-fin.MF], Feb 2016. 72, 74, 82

[RJDDan16] Sammy Ragy, Marcin Jarzyna, and Rafał Demkowicz-Dobrzański. Compatibility in multiparameter quantum metrology. *Phys. Rev. A*, 94:052108, Nov 2016. 122

[RM10] Soumya Singha Roy and T.S. Mahesh. Density matrix tomography of singlet states. *Journal of Magnetic Resonance*, 206(1):127 – 133, 2010. 45

[Ros10] Sheldon Ross. *A first course in probability.* Pearson, 8th ed., 2010. 5, 72, 74, 98, 99, 104, 110, 111, 113, 143, 144

[Rov04] Carlo Rovelli, editor. *Quantum gravity.* Cambridge university press, 2004. 107

[Roy68] H. L. Royden. *Real Analysis.* The Macmillan company, Second ed., 1968. 74, 78, 132

[RTB+16] Irina V. Rasina, Ekaterina A. Trushkova, Olga V. Baturina, Alexander V. Bulatov, and Irina S. Guseva. Development and applications of krotov method of global control improvement. *AIP Conference Proceedings*, 1738(1):400009, 2016. 15

[Rud76] Walter Rudin. *Principles of mathematical analysis.* McGraw Hill, Third ed., 1976. 74, 75

[SAL13] L. Chua S. Aaronson, A. Bouland and G. Lowther. *arXiv*, 1303.2834v3 [quant-ph], 2013.

[SBA17] Jaskaran Singh, Kishor Bharti, and Arvind. Quantum key distribution protocol based on contextuality monogamy. *Phys. Rev. A*, 95:062333, Jun 2017. 21

[SBB+08] Daniel Salart, Augustin Baas, Cyril Branciard, Nicolas Gisin, and Hugo Zbinden. Testing the speed of 'spooky action at a distance'. *Nature*, 454:861, 2008. 1, 2

[SCW+12] Hong-Yi Su, Jing-Ling Chen, Chunfeng Wu, Sixia Yu, and C. H. Oh. Quantum contextuality in a one-dimensional quantum harmonic oscillator. *Phys. Rev. A*, 85:052126, May 2012. 21, 22, 24, 25, 29, 30

[Sha08] R Shankar. *Principles of Quantum Mechanics*. Springer, 2008. 6, 7, 72, 76

[SHC00] Yehuda Sharf, Timothy F. Havel, and David G. Cory. Spatially encoded pseudopure states for nmr quantum-information processing. *Phys. Rev. A*, 62:052314, Oct 2000. 16

[SHHC87] Tycho Sleator, Erwin L. Hahn, Claude Hilbert, and John Clarke. Nuclear-spin noise and spontaneous emission. *Phys. Rev. B*, 36:1969–1980, Aug 1987. 12

[SJK+10] Stephanie Simmons, Jonathan A. Jones, Steven D. Karlen, Arzhang Ardavan, and John J. L. Morton. Magnetic field sensors using 13-spin cat states. *Phys. Rev. A*, 82:022330, Aug 2010. 51

[SK17] C S Sudheer Kumar. *Young Quantum-2017 (Conference)*. Harish-Chandra Research Institute, 2017. 84

[SK19] C. S. Sudheer Kumar. Violation of space–time bell-chsh inequality beyond the tsirelson bound and quantum cryptography. *Pramana*, 93(5):67, Aug 2019. viii, 85

[SKBSS20] C S Sudheer Kumar, A Biswas, A Sen(De), and U Sen. Frequentist-approach inspired theory of quantum random phenomena predicts signaling. *arXiv*, 1903.12096v2 [quant-ph], Oct 2020. viii, 4, 5, 6, 12, 73, 86

[SKM18] C. S. Sudheer Kumar and T. S. Mahesh. Ancilla-induced amplification of quantum fisher information. *The European Physical Journal Plus*, 133(11):460, Nov 2018. viii, 49

[SMO12] A. Seijas-Macias and A. Oliveira. *Probability and Statistics*, 32:87, 2012. 143

[SMP88] D. Suter, K. T. Mueller, and A. Pines. Study of the aharonov-anandan quantum phase by nmr interferometry. *Phys. Rev. Lett.*, 60:1218–1220, Mar 1988. 34

[Soh06] Houshang H Sohrab. *Basic real analysis*. Springer (India) pvt. ltd., Springer international edition (2006). 74, 78, 132

[Son06] Dieter Sondermann. *Introduction to Stochastic Calculus for Finance*. Springer-Verlag Berlin Heidelberg, 2006. 4, 72, 82, 105, 115

[SP00] P W. Shor and J Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000. 87

[SP19] Paul Vincent Spade and Claude Panaccio. William of ockham. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, spring 2019 edition, 2019.

[Spa13] Aris Spanos. A frequentist interpretation of probability for model-based inductive inference. *Synthese*, 190(9):1555–1585, Jun 2013. 72, 105

[SR08] V Scarani and R Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008. 87

[SRM13] Abhishek Shukla, K. Rama Koteswara Rao, and T. S. Mahesh. Ancilla-assisted quantum state tomography in multiqubit registers. *Phys. Rev. A*, 87:062317, Jun 2013. xvii, 16, 53, 54, 57, 58

[SSM14] Abhishek Shukla, Manvendra Sharma, and T S Mahesh. Noon states in star-topology spin-systems: Applications in diffusion studies and rf inhomogeneity mapping. *Chemical Physics Letters*, 592(Supplement C):227 – 231, 2014. 51

[SSS13] H A Shenoy, R Srikanth, and T Srinivas. Semi-counterfactual cryptography. *Eur. phy. Lett.*, 103(6):60008, sep 2013. 87

[ST05] Y S.Chow and H Teicher. *Probability theory: Independence, interchangeability, martingales.* Springer Verlag, Third ed., 2005. 72, 74, 75, 104, 113

[Sto15] Cristi Stoica. The tao of it and bit. *arXiv*, 1311.0765v2 [quant-ph], Aug 2015. 1, 2

[STP⁺16] R D Sharma, K Thapliyal, A Pathak, A K Pan, and A De. Which verification qubits perform best for secure communication in noisy channel? *Quant. Info. Proc.*, 15(4):1703–1718, Apr 2016. 87

[STZG00] Valerio Scarani, Wolfgang Tittel, Hugo Zbinden, and Nicolas Gisin. The speed of quantum information and the preferred frame: analysis of experimental data. *Physics Letters A*, 276:1–7, 2000. 1, 2

[SW10]   Y Sun and Q Y Wen. Counterfactual quantum key distribution with high efficiency. *Phys. Rev. A*, 82:052318, Nov 2010. 87

[TA14]   Geza Toth and Iagoba Apellaniz. Quantum metrology from a quantum information science perspective. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424006, 2014. 7, 50, 51, 56, 59, 61

[TH06]   J. Tolar and P. Hájícek. Can differently prepared mixed states be distinguished? *Physics Letters A*, 353(1):19 – 23, 2006. 76, 84

[TNA16] M M Taddei, R V Nery, and L Aolita. Necessary and sufficient conditions for multipartite bell violations with only one trusted device. *Phys. Rev. A*, 94:032106, Sep 2016. 94

[TPB17] K Thapliyal, A Pathak, and S Banerjee. Quantum cryptography over non-markovian channels. *Quant. Info. Proc.*, 16(5):115, Mar 2017. 87

[vL96]   Michiel van Lambalgen. *Randomness and foundations of probability: von Mises' axiomatisation of random sequences*, volume Volume 30 of *Lecture Notes–Monograph Series*, pages 347–367. Institute of Mathematical Statistics, Hayward, CA, 1996. 127

[VM81]   R. Von Mises. *Probability, Statistics, and Truth.* Dover Books on Mathematics Series. Dover Publications, 1981. 72

[vN55]   John von Neumann. *Mathematical foundations of quantum mechanics.* Princeton university press, 1955. 2, 6, 33, 37, 42

[vN76]   John von Neumann. *John von Neumann collected works Vol. III, chapter 6 "On infinite direct products".* Pergamon press, 1976. 129

[VS12]   Paolo Vicig and Teddy Seidenfeld. Bruno de finetti and imprecision: Imprecise probability does not exist! *International Journal of Approximate Reasoning*, 53(8):1115 – 1123, 2012. Imprecise Probability: Theories and Applications (ISIPTA'11). 115

[VV14]   U Vazirani and T Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014. 87

[WB12]   J. J. Wallman and S. D. Bartlett. *arXiv*, 1005.2438v3 [quant-ph], 2012. 112

[WGFVB97] J Wrachtrup, A Gruber, L Fleury, and C Von Borczyskowski. Magnetic resonance on single nuclei. *Chemical physics letters*, 267(1-2):179–185, 1997. 50

[Wil10]   D. Williams. *Weighing the Odds: A Course in Probability and Statistics*. Cambridge, 2010. 72, 74, 105, 113

[WJD07]   H M Wiseman, S J Jones, and A C Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Phys. Rev. Lett.*, 98:140402, Apr 2007. 94

[WTY06]   E Waks, H Takesue, and Y Yamamoto. Security of differential-phase-shift quantum key distribution against individual attacks. *Phys. Rev. A*, 73:012344, Jan 2006. 87

[WVEB06] Herbert Walther, Benjamin T H Varcoe, Berthold-Georg Englert, and Thomas Becker. Cavity quantum electrodynamics. *Rep. Prog. Phys.*, 69, Jul 2006. 21

[WZ82]   W K Wootters and W H Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. 4

[WZ83] John Archibald Wheeler and Wojciech Hubert Zurek. *Quantum Theory and Measurement.* Princeton university press, 1983. vi, 1, 2

[YCY+16] H L Yin, T Y Chen, Z W Yu, H Liu, L X You, Y B Zhou, S J Chen, Y Mao, M Q Huang, W J Zhang, H Chen, M J Li, D Nolan, F Zhou, X Jiang, Z Wang, Q Zhang, X B Wang, and J W Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, Nov 2016. 87

[YLC+10] Z Q Yin, H W Li, W Chen, Z F Han, and G C Guo. Security of counterfactual quantum cryptography. *Phys. Rev. A*, 82:042335, Oct 2010. 87

[YNSA17] Rozhin Yousefjani, Rosanna Nichols, Shahriar Salimi, and Gerardo Adesso. Estimating phase with a random generator: Strategies and resources in multiparameter quantum metrology. *Phys. Rev. A*, 95:062307, Jun 2017. 62, 66, 123

[ZSM+13] Wei Zhong, Zhe Sun, Jian Ma, Xiaoguang Wang, and Franco Nori. Fisher information under decoherence in bloch representation. *Phys. Rev. A*, 87:022337, Feb 2013. 56, 61, 62, 120