

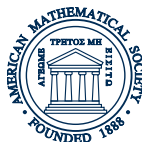
CONTEMPORARY MATHEMATICS

482

Advances in Quantum Computation

Representation Theory, Quantum Field Theory,
Category Theory, Mathematical Physics,
and Quantum Information Theory
September 20–23, 2007
University of Texas at Tyler

Kazem Mahdavi
Deborah Koslover
Editors



This page intentionally left blank

CONTEMPORARY MATHEMATICS

482

Advances in Quantum Computation

Representation Theory, Quantum Field Theory,
Category Theory, Mathematical Physics,
and Quantum Information Theory
September 20–23, 2007
University of Texas at Tyler

Kazem Mahdavi
Deborah Koslover
Editors



American Mathematical Society
Providence, Rhode Island

Editorial Board

Dennis DeTurck, managing editor

George Andrews Abel Klein Martin J. Strauss

2000 *Mathematics Subject Classification*. Primary 81P68, 81T18, 81V10, 68M07, 37F25, 20F36, 57M25, 57M27, 47N55.

Library of Congress Cataloging-in-Publication Data

Conference on Representation Theory, Quantum Field Theory, Category Theory, and Quantum Information Theory (2007 : University of Texas at Tyler)

Advances in quantum computation : a conference on representation theory, quantum field theory, category theory, mathematical physics and quantum information theory, September 20–23, 2007, University of Texas at Tyler / Kazem Mahdavi, Deborah Koslover, editors.

p. cm. — (Contemporary mathematics ; v. 482)

Includes bibliographical references.

ISBN 978-0-8218-4627-8 (alk. paper)

1. Quantum computers—Congresses. 2. Quantum theory—Congresses. 3. Quantum communication—Congresses. I. Mahdavi, Kazem. II. Koslover, Deborah. III. Title.

QA76.889.C66 2007

004.1—dc22

2008042590

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 2009 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.

Copyright of individual articles may revert to the public domain 28 years
after publication. Contact the AMS for copyright status of individual articles.

Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 14 13 12 11 10 09

Contents

Preface	v
List of Participants	vii
Mathematical Formulations of Atom Trap Quantum Gates Z. ZHANG and G. CHEN	1
Charge Renormalization, Apéry’s Number, and the Trefoil Knot H.E. BRANDT	23
Braid Group, Temperley–Lieb Algebra, and Quantum Information and Computation Y. ZHANG	49
Poisson Algebras and Yang-Baxter Equations T. SCHEDLER	91
Ambiguity in Quantum-theoretical Descriptions of Experiments J.M. MYERS and F.H. MADJID	107
Reference Frame Fields based on Quantum Theory Representations of Real and Complex Numbers P. BENIOFF	125
Two Paradigms for Topological Quantum Computation E.C. ROWELL	165
Contraction of Matchgate Tensor Networks on Non-planar Graphs S. BRAVYI	179
Probing Topological Order in Quantum Hall States Using Entanglement Calculations M. HAQUE	213
Topological Order and Entanglement A. HAMMA	219
Hierarchical Quantum Search V.E. KOREPIN and Y. XU	225

This page intentionally left blank

Preface

The 2007 Conference on Representation Theory, Quantum Field Theory, Category Theory, and Quantum Information Theory, held September 20 - 23 at the University of Texas at Tyler, was funded by the NSF for the purpose of bringing together scientists from a wide range of fields to share research and stimulate new ideas. Attendees included mathematicians, physicists, and computer scientists. Speakers came from major industries including IBM; major national laboratories including the Army Research Lab, Los Alamos and Argonne National Lab; and major education institutions including MIT, Harvard, and Stanford.

Our main purpose in publishing this proceedings is to bring together papers from a wide spectrum of disciplines to stimulate progress in the field of computation and communication, in particular, quantum communication (QC). The eleven contributed papers included in this volume cover a wide range of topics related to QC, including physical aspects, mathematical aspects and foundational issues of QC. All submissions were peer reviewed and the most outstanding have been chosen to appear here.

It is generally believed that there is a hierarchy of abstraction in the fields of Computer Science and Engineering, the Sciences, and Mathematics, with one end of the spectrum addressing real world problems and the other end concerned with more abstract, less practical issues. This leads to scientists in different fields reading and publishing in different journals and attending different conferences. Work done in one field may remain completely unknown in another. This compartmentalization of knowledge slows the advancement of science and leads to needless duplication of effort. By bringing together scientists who study QC in a wide range of fields and settings, we hope to generate cross-pollination of ideas and stimulate research in the field. We hope this volume will lead to advances in QC.

The editors would like to thank our co-organizers, Louis Kauffman (UIC) and Samuel Lomonaco (UMBC), of the Conference on Representation Theory, Quantum Field Theory, Category Theory, and Quantum Information Theory. We would also like to thank our speakers: John Armstrong (Tulane), Howard Barnum (LANL), Paul Benioff (ANL), Howard Brandt (ARL), Sergey Bravyi (IBM), Gavin Brenner (Innsbrook), Goong Chen (TAMU), Alioscia Hamma (USC), Masud Haque (MPI), Louis Kauffman (UIA), Eun-Ah Kim (Stanford), Vladimir Korepin (Stony Brook), Samuel Lomonaco (UMBC), John M. Myers (Harvard), Eric Rowell (TAMU), Travis Schedler (Chicago), Peter Shore (MIT) and Yong Zhang (Utah). Finally, the editors would like to thank the NSF for funding the conference (DMS 0703900).

Kazem Mahdavi
Deborah Koslover

This page intentionally left blank

List of Participants

John Armstrong
Tulane University

Howard Barnum
Los Alamos National Laboratory

Paul Benioff
Argonne National Laboratory

Howard Brandt
Army Research Laboratory

Sergey Bravyi
IBM Research

Gavin Brennen
Institute of Quantum Optics and
Quantum Information

Stephen Bullock
Institute Defense Analyses,
Center for Computing Science

Goong Chen
Texas A&M University

Alioscia Hamma
University of Southern California

Masudul Haque
Max Planck Institute

Louis Kauffman
University of Illinois at Chicago

Eun-Ah Kim
Stanford University

Vladimir Korepin
C.N. Yang Institute for Theoretical
Physics,
SUNY, Stony Brook

Deborah Koslover
University of Texas at Tyler

Samuel Lomonaco
University of Maryland, Baltimore
County

Kazem Mahdavi
University of Texas at Tyler

John Myers
Harvard University

Eric Rowell
Texas A&M University

Travis Schedler
University of Chicago
Massachusetts Institute of Technology

Melinda Schulteis
Concordia University, Irvine

Peter Shor
Massachusetts Institute of Technology

Yong Zhang
University of Utah
University of Central Florida

This page intentionally left blank

Mathematical Formulations of Atom Trap Quantum Gates

Zhigang Zhang and Goong Chen

ABSTRACT. Neutral atom traps constitute a good candidate for quantum computing devices due to their advantages of having long coherence time, scalability and available technology to trap and cool them. There are three major proposals for atom traps as quantum gates: optical lattices, focused laser traps and static magnetic traps. Existing literature is mostly written by physicists and rigorous mathematical derivations appear to be incomplete. In this paper, we address the optical lattices proposal by giving a sufficiently self-contained mathematical study of the universality of such 1-bit and 2-bit quantum gates. A proper physics background is described. The setup of qubits and the proofs of universality are given based on Rabi rotations, induced dipole-dipole interactions and atom collisions.

1. Introduction

Quantum computing, since its inception during the 1980s, has made giant strides in both theory and experiments. A quantum computer executes commands via the hardware of quantum gates. Liquid NMR (nuclear magnetic resonance) was first used as proof of principle to demonstrate the feasibility of quantum computing by Gerschenfeld and Chuang, and Cory, Fahmy, and Havel (see, e.g. [9, 11]) during the 1990s. Since then, tremendous progress has been made in the proposals, designs and experiments for a variety of quantum devices made of ion traps, cavity QED, quantum dots, atom traps, linear optics, superconducting quantum interference devices, solid-state NMR, etc. See [7]. Efforts are underway to improve their fidelity.

A quantum system suitable for quantum computation must meet many requirements. Information is encoded in the state of a quantum system, and manipulated with laser pulses or other electromagnetic fields. Before the computation, the system needs to be initialized to a certain state, normally the ground state. This process is called initialization. Decoherence and dissipation pose great difficulties for quantum computation. They cause information “leak” and makes the computation not reliable. Unfortunately, they are inevitable. The operations must be fast enough so that the computation can be completed before the system loses its coherence. Carefully designed fault tolerant algorithms and error-correction codes are needed to counter the effects of decoherence and dissipation. (This will not

1991 *Mathematics Subject Classification.* 68M07, 81V80.

Key words and phrases. Quantum computation, neutral atom traps, optical lattices, universal quantum gates.

be included in this paper.) After the computation, results are retrieved through measurements.

In this paper, we will discuss mainly *neutral atom trap quantum gates using optical lattices*. Neutral atoms constitute a good candidate for quantum computing devices. They have long coherence time, existing technology to trap and cool them to ground state, and potential for scalability [2, 4, 6, 12]. The same technology used to cool atoms can be used to trap them in a three dimensional lattice. The weak interaction between a neutral atom and its environment, normally electric and magnetic fields, gives the atom long coherence time and makes its evolution robust with respect to external fields. However, this weak interaction also makes it difficult to entangle two atoms, namely, the implementation of 2-qubits entangling operations. Although 1-qubit operations can be realized with laser pulses or other methods, 2-qubit operations need controlled interactions between arbitrary two atoms, or at least two neighboring atoms. There are many proposals for trapping atoms in space and entangling two atoms. In this article, we will limit our study to neutral atoms trapped in optical lattices, and two major methods for entangling two atoms: induced dipole-dipole interaction, and controlled cold atom collisions.

For the sake of future needs in this paper, we first state the following universality theorem [7, Section 2.6] due to J.-L. Brylinski and R. Brylinski [5]. It refines a universality theorem originally due to DiVincenzo [1, 13].

THEOREM 1.1. *The collection of all the 1-qubit gates $U_{\theta,\phi}$, $0 \leq \theta, \phi \leq 2\pi$, together with the 2-qubit CNOT gate, is universal, where $U_{\theta,\phi}$ is defined by*

$$(1) \quad U_{\theta,\phi} = \begin{bmatrix} \cos \theta & -ie^{-i\phi} \sin \theta \\ -ie^{-i\phi} \sin \theta & \cos \theta \end{bmatrix}.$$

□

The rest of this paper is divided into two sections. We start with a brief introduction about the $\text{lin} \perp \text{lin}$ configuration in Subsection 2.1. Then in Subsection 2.2, we show how potential wells move in space when the angle between the polarization directions of the two light beams changes. In Subsection 2.3, the potentials of two types of atoms with different Zeeman states are given. In Section 3, we set up qubits and consider 1-qubit and 2-qubit operations. The 1-qubit Rabi rotations are derived in Subsection 3.1. Two-qubit entanglement can be realized in two ways: induced dipole-dipole interactions (Subsection 3.2) and cold atom collisions (Subsection 3.3).

2. Optical lattices

An optical lattice consists of a set of periodic potentials spaced in wavelength size, created by a set of interfering laser beams in such a way that they can trap and cool atoms. A lattice can be of one, two or three dimensions. The basic configuration is the one-dimensional lattice usually formed by two counter-propagating beams. In laser cooling and trapping, an important feature is that the interference of two laser beams depends on their mutual polarization. *Polarization gradient* can be used to displace two sets of atoms in different Zeeman states relative to each other. In order to form a strong polarization gradient, two counter-propagating laser beams with different linear polarization directions are used and the setup is

called a *linθlin configuration*. When the angle between the two polarization directions, θ , is $\pi/2$, it is called a *lin ⊥ lin configuration*. This configuration is used in the laser cooling and trapping.

The lin ⊥ lin configuration just mentioned is not the only way to form an optical lattice and to trap atoms. For example, a two-dimensional double well lattice can be realized with a single folded, retro-reflected beam [19]. Some experiment has been reported in transporting atoms using that setup [8].

2.1. The lin ⊥ lin configuration. Two counter-propagating laser beams with the same frequency and amplitude form a standing wave along the direction of propagation. Moreover, if both beams are linearly polarized and their polarization vectors are mutually perpendicular, they form a polarization gradient and the polarization changes periodically in a certain way in space. Without loss of generality, we assume that both light beams travel along the z -axis with polarization vectors \mathbf{e}_1 and \mathbf{e}_2 , respectively, see (3) below, and their phases are zero. Then the electric fields of the two lasers are given as

$$(2) \quad \begin{aligned} \mathbf{E}_1(z, t) &= \frac{1}{2}\epsilon_1 \mathbf{e}_1 e^{-i(\omega t - kz)} + c.c. \\ \mathbf{E}_2(z, t) &= \frac{1}{2}\epsilon_2 \mathbf{e}_2 e^{-i(\omega t + kz)} + c.c. \end{aligned}$$

respectively, where *c.c.* means the complex conjugate of the preceding terms. Two vectors \mathbf{e}_1 and \mathbf{e}_2 are defined as following:

$$(3) \quad \begin{aligned} \mathbf{e}_1 &= \frac{1}{\sqrt{2}}(\mathbf{e}_x + \mathbf{e}_y), \\ \mathbf{e}_2 &= \frac{1}{\sqrt{2}}(\mathbf{e}_x - \mathbf{e}_y). \end{aligned}$$

Let $\epsilon_1 = \epsilon_2 = \epsilon$; the total electric field at z is the sum of $\mathbf{E}_1(z, t)$ and $\mathbf{E}_2(z, t)$:

$$(4) \quad \mathbf{E}(z, t) = \frac{1}{2}\epsilon e^{-i\omega t}(\mathbf{e}_1 e^{ikz} + \mathbf{e}_2 e^{-ikz}) + c.c.$$

In terms of \mathbf{e}_x and \mathbf{e}_y , the above can be rewritten as

$$(5) \quad \mathbf{E}(z, t) = \frac{1}{2}\epsilon\sqrt{2}e^{-i\omega t}(\mathbf{e}_x \cos(kz) + i\mathbf{e}_y \sin(kz)) + c.c.$$

Equation (5) shows how the polarization changes along z axis. At $z = 0, \lambda/2, \lambda, 3\lambda/2, \dots$, where $\lambda = 2\pi/k$, the polarization is linear along \mathbf{e}_x . At $z = \lambda/4, 3\lambda/4, 5\lambda/4, 7\lambda/4, \dots$, the polarization is linear along \mathbf{e}_y . However, at $z = \lambda/8, 5\lambda/8, 9\lambda/8, 13\lambda/8, \dots$,

$$(6) \quad \mathbf{E}(z, t) = \pm \frac{1}{2}\epsilon e^{-i\omega t}(\mathbf{e}_x + i\mathbf{e}_y) + c.c.$$

and the field has a left circular polarization (σ^+). At $z = 3\lambda/8, 7\lambda/8, 11\lambda/8, 15\lambda/8, \dots$,

$$(7) \quad \mathbf{E}(z, t) = \pm \frac{1}{2}\epsilon e^{-i\omega t}(\mathbf{e}_x - i\mathbf{e}_y) + c.c.$$

and the field has a right circular polarization (σ^-). This is shown in Fig. 1.

Vectors \mathbf{e}_x and \mathbf{e}_y are on the x - y plane, corresponding to two linear polarization directions. The total electric field can also be expressed as the combination of two circularly polarized light beams. Take \mathbf{e}_+ and \mathbf{e}_- as a set of basis, defined by

$$(8) \quad \begin{aligned} \mathbf{e}_+ &= -\frac{1}{\sqrt{2}}(\mathbf{e}_x + i\mathbf{e}_y), \\ \mathbf{e}_- &= \frac{1}{\sqrt{2}}(\mathbf{e}_x - i\mathbf{e}_y). \end{aligned}$$

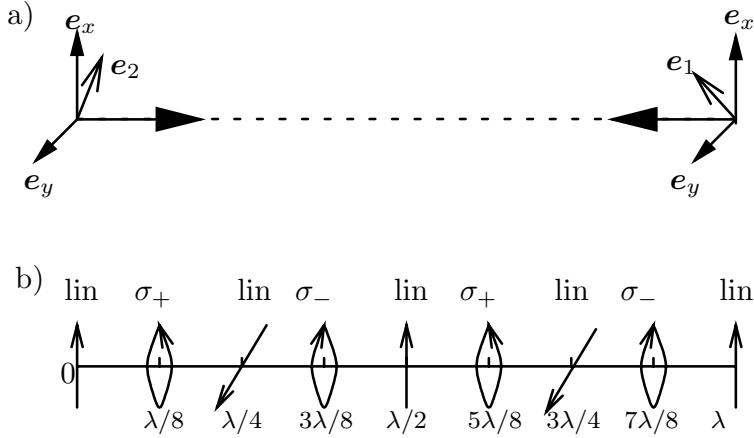


FIGURE 1. A schematic of the $\text{lin} \perp \text{lin}$ configuration. (a). Two linearly polarized counter-propagating laser beams form a standing wave. The polarization vectors of the two laser beams are perpendicular to each other. (b). The polarization changes along the z axis. It is called polarization gradient.

Then we can rewrite $\mathbf{E}(z, t)$ as

(9)

$$\begin{aligned} \mathbf{E}(z, t) &= \frac{1}{2} \epsilon e^{-i\omega t} ((-\mathbf{e}_+ + \mathbf{e}_-) \cos(kz) + (-\mathbf{e}_+ - \mathbf{e}_-) \sin(kz)) + c.c. \\ &= \frac{1}{2} \epsilon e^{-i\omega t} (-\mathbf{e}_+ (\cos(kz) + \sin(kz)) + \mathbf{e}_- (\cos(kz) - \sin(kz))) + c.c. \\ &= \frac{1}{2} \epsilon e^{-i\omega t} (-\sqrt{2} \mathbf{e}_+ \cos(kz - \frac{\pi}{4}) + \sqrt{2} \mathbf{e}_- \sin(\frac{\pi}{4} - kz)) + c.c. \end{aligned}$$

Note that \mathbf{e}_+ and \mathbf{e}_- correspond to left circular and right circular polarization, respectively. When $kz - \frac{\pi}{4} = n\pi$ where n is an integer, the amplitude of the left circular part attains its peak and the field is purely left circularly polarized. Similarly, when $\frac{\pi}{4} - kz = m\pi + \frac{\pi}{2}$ for an integer m , the field is purely right circularly polarized.

If \mathbf{e}_1 and \mathbf{e}_2 in (3) are replaced by

$$\begin{aligned} \mathbf{e}_1 &= \mathbf{e}_x, \\ \mathbf{e}_2 &= -i\mathbf{e}_y, \end{aligned} \quad (10)$$

$\mathbf{E}(z, t)$ will be given by

$$\mathbf{E}(z, t) = \frac{\sqrt{2}}{2} \epsilon e^{-i\omega t} (\mathbf{e}_- \cos(kz) - i \mathbf{e}_+ \sin(kz)) + c.c. \quad (11)$$

2.2. The $\text{lin}\theta\text{lin}$ configuration. The $\text{lin}\theta\text{lin}$ configuration is a generalization of the $\text{lin} \perp \text{lin}$ configuration. A $\text{lin}\theta\text{lin}$ configuration consists of two counter-propagating linearly polarized laser beams along the z axis, except that the angle between the two polarization vectors can be arbitrary and are not necessary perpendicular to each other. A standing wave is formed which shows periodic polarization gradient along the propagating direction, say, the z -axis. The positions where the left and right circular polarizations attain their peak amplitude move when the



FIGURE 2. The lin θ lin configuration is similar to the lin \perp lin configuration except that the angle between the two polarization vectors is tunable.

angle changes. If the potential of a particle is dominated by the intensity of the left or right circularly polarized light, the potential wells also moves along the z -axis.

We assume \mathbf{E}_1 and \mathbf{E}_2 given as before, except that we replace \mathbf{e}_1 and \mathbf{e}_2 by

$$(12) \quad \begin{aligned} \mathbf{e}_1 &= \mathbf{e}_x \cos(\frac{\theta}{2}) + \mathbf{e}_y \sin(\frac{\theta}{2}), \\ \mathbf{e}_2 &= \mathbf{e}_x \cos(\frac{\theta}{2}) - \mathbf{e}_y \sin(\frac{\theta}{2}). \end{aligned}$$

This configuration is shown in Fig. 2. The resulting electric field in terms of \mathbf{e}_x and \mathbf{e}_y at z is then given by

$$(13) \quad \begin{aligned} \mathbf{E}(z, t) &= \mathbf{E}_1 + \mathbf{E}_2 \\ &= \frac{1}{2}\epsilon e^{-i\omega t}(\mathbf{e}_1 e^{ikz} + \mathbf{e}_2 e^{-ikz}) + c.c. \\ &= \frac{1}{2}\epsilon e^{-i\omega t}(2\mathbf{e}_x \cos(\frac{\theta}{2}) \cos(kz) + 2i\mathbf{e}_y \sin(\frac{\theta}{2}) \sin(kz)) + c.c. \end{aligned}$$

Using (8), we can also write $\mathbf{E}(z, t)$ in terms of the circular polarization vectors \mathbf{e}_+ and \mathbf{e}_- :

$$(14) \quad \begin{aligned} \mathbf{E}(z, t) &= \frac{\sqrt{2}}{2}\epsilon e^{-i\omega t}((- \mathbf{e}_+ + \mathbf{e}_-) \cos(\frac{\theta}{2}) \cos(kz) + (- \mathbf{e}_+ - \mathbf{e}_-) \sin(\frac{\theta}{2}) \sin(kz)) + c.c. \\ &= \frac{\sqrt{2}}{2}\epsilon e^{-i\omega t}(- \mathbf{e}_+ \cos(kz - \frac{\theta}{2}) + \mathbf{e}_- \cos(kz + \frac{\theta}{2})) + c.c. \end{aligned}$$

Let $A_+ = -\sqrt{2}\epsilon \cos(kz - \frac{\theta}{2})$ and $A_- = \sqrt{2}\epsilon \cos(kz + \frac{\theta}{2})$. Then we get

$$(15) \quad \mathbf{E}(z, t) = \frac{1}{2}(A_+ \mathbf{e}_+ + A_- \mathbf{e}_-) e^{-i\omega t} + c.c.,$$

where A_+ and A_- are the amplitudes of the left and right circularly polarized parts, respectively. When $\theta = \pi/2$, (14) is reduced to (9), the lin \perp lin case. Peak values of $|A_+|$ occur at $z = \frac{m}{2}\lambda + \frac{\theta}{2k}$, where m is an integer and $\lambda = \frac{2\pi}{k}$, while those of $|A_-|$ occur at $z = \frac{m}{2}\lambda - \frac{\theta}{2k}$. We are only concerned with $\theta \in [0, \pi/2]$. If θ is in that interval, the distance between two neighboring peaks of $|A_+|$ and $|A_-|$ can be calculated as θ/k . When $\theta = 0$, the field is linearly polarized everywhere. When $\theta = \pi/2$, the distance is maximized.

2.3. Interactions between a neutral atom and a standing wave. Analysis of the optical pumping, energy shift, and cooling of a general atom in a laser field is tedious and complicated. Fortunately, it can be greatly simplified under certain assumptions. In this subsection, we will limit our discussion under several such assumptions:

- (i) we assume that the wavelength of the laser is much larger than the size of the atom;

- (ii) the atoms we discussed are assumed to be deeply cooled, and they are trapped in a potential well;
- (iii) the laser we use has low enough intensity that the low saturation limit holds.

2.3.1. *The Hamiltonian of a neutral atom in a standing wave.* Sub-levels of the ground level of an atom are degenerate without an external field. These sub-levels, called *Zeeman sub-levels*, have *different angular momenta*. If we put the atom in a static magnetic field, these Zeeman sub-levels split and the atom loses its degeneracy. This degeneracy can also be removed when the atom is put in an oscillating electric field such as a laser field due to the *ac-Stark shift*, an energy shift proportional to the intensity of the laser. This energy shift is extremely important here since it forms the basis of atom trapping and manipulation. In the following, we show the derivation of the ac-Stark shift of an atom with multiple sub-levels by following the work of Cohen-Tannoudji [10]. Fine details are omitted and the interested readers are referred to the original literature.

Consider an atom with two levels, a ground state g and an excited state e . The ground state consists of $2J_g + 1$ sub-levels, denoted by $|J_g\mu\rangle$, $\mu = -J_g, -J_g + 1, \dots, J_g$, respectively. Similarly, the excited state consists of $2J_e + 1$ sub-levels, denoted by $|J_em\rangle$, where $m = -J_e, \dots, J_e$. Define P_e and P_g to be the projection operators onto the ground level and excited level, respectively. They are given as

$$(16) \quad \begin{aligned} P_g &= \sum_{\mu=-J_g}^{J_g} |J_g\mu\rangle\langle J_g\mu|, \\ P_e &= \sum_{m=-J_e}^{J_e} |J_em\rangle\langle J_em|. \end{aligned}$$

Let σ be the density operator of the atom. Then

$$(17) \quad \sigma = \sigma_{gg} + \sigma_{ge} + \sigma_{eg} + \sigma_{ee},$$

where $\sigma_{ab} = P_a\sigma P_b$, $a, b = e, g$. Obviously, σ_{ge} and σ_{eg} are off-diagonal block matrix elements of σ and they represent the coherence of an atom between e and g .

With the complex conjugate expressed explicitly, the electric field at z can be written as

$$(18) \quad \mathbf{E}(z, t) = \mathbf{E}^+(z)e^{-i\omega t} + \mathbf{E}^-(z)e^{i\omega t},$$

where $\mathbf{E}^+ = \frac{1}{2}\epsilon\mathbf{e}$ with \mathbf{e} being the polarization vector of the field and ϵ its amplitude, and ω the frequency of the laser. The Hamiltonian of an atom in the field consists of two terms:

$$(19) \quad H = H_A + H_{AL}$$

where H_A is the *atom's Hamiltonian without the external field* and H_{AL} is the *interaction Hamiltonian*. They are given by

$$(20) \quad \begin{aligned} H_A &= \hbar\omega_A P_e, \\ H_{AL} &= -\mathbf{d}^+ \cdot \mathbf{E}^+(z)e^{-i\omega t} - \mathbf{d}^- \cdot \mathbf{E}^-(z)e^{i\omega t}, \end{aligned}$$

where $\hbar\omega_A$ is the energy difference between the ground and the excited levels. The operators \mathbf{d}^+ and \mathbf{d}^- are defined in terms of P_g , P_e , and the electric dipole moment operator \mathbf{d} :

$$(21) \quad \begin{aligned} \mathbf{d}^+ &= P_e \mathbf{d} P_g, \\ \mathbf{d}^- &= P_g \mathbf{d} P_e. \end{aligned}$$

A rotating wave approximation has been used in (20) [18, Section 5.2].

2.3.2. *The Clebsch-Gordan coefficients and Wigner-Eckart theorem.* Assume that \mathbf{J}_1 and \mathbf{J}_2 are two angular momenta and \mathbf{J} is their sum. We denote the eigenvalues of J_1^2 , J_2^2 , and J^2 as $j_1(j_1 + 1)$, $j_2(j_2 + 1)$, and $j(j + 1)$, respectively. Similarly, the projection operators along the z -axis are denoted J_{1z} , J_{2z} , and J_z , respectively. Since J_1^2 commutes with J_{1z} , a group of simultaneous eigenvectors of J_1^2 and J_{1z} can be found and denoted as $|J_1 m_1\rangle$, where $m_1 = -j_1, -j_1 + 1, \dots, j_1 - 1, j_1$. By defining

$$(22) \quad J_{1\pm} = j_{1x} \pm i j_{1y},$$

we have

$$(23) \quad J_{1\pm}|j_1 m_1\rangle = \sqrt{(j_1 \mp m_1)(j_1 \pm m_1 + 1)}|j_1, m_1 \pm 1\rangle.$$

Similarly, J_2^2 and J_{2z} have a group of simultaneous eigenvectors $|j_2 m_2\rangle$, where $m_2 = -j_2, -j_2 + 1, \dots, j_2 - 1, j_2$, and we can also define $J_{2\pm}$ as above.

All the possible products of $|j_1 m_1\rangle$ and $|j_2 m_2\rangle$, which could be simply written as $|m_1 m_2\rangle$ since j_1 and j_2 are known and fixed, form a basis of the wavefunction space. There are a total of $(2j_1 + 1)(2j_2 + 1)$ of such eigenvectors. Although J^2 does not commute with J_{1z} and J_{2z} , it commutes with J_1^2 , J_2^2 , and J_z . A group of simultaneous eigenvectors can also be found for J^2 , J_1^2 , J_2^2 , and J_z , and they constitute another basis. Neglecting the quantum number J_1^2 and J_2^2 , we denote an eigenvector from this basis as $|jm\rangle$, where $m = -j, -j + 1, \dots, j - 1, j$. A triangle relation applies to j_1 , j_2 , and j :

$$|j_1 - j_2| \leq j \leq j_1 + j_2,$$

and a simple calculation shows that the total number of eigenvectors in the last basis is also $(2j_1 + 1)(2j_2 + 1)$.

Both $|jm\rangle$ and $|m_1 m_2\rangle$ are bases of the same finite-dimensional space, and every $|jm\rangle$ is a linear combination of $|m_1 m_2\rangle$:

$$(24) \quad |jm\rangle = \sum_{m_1, m_2} \langle m_1 m_2 | jm \rangle |m_1 m_2\rangle.$$

The coefficients in front of $|m_1 m_2\rangle$ in the summation above are known as the *Clebsch-Gordan coefficients* (C-G coefficients), also noted as $\langle j_1 m_1 j_2 m_2 | j_1 j_2 j m \rangle$ if both J_1^2 and J_2^2 are explicitly listed. The C-G coefficients vanish unless $m = m_1 + m_2$ and j satisfies the triangle relation. By choosing proper phases for the two groups of eigenvectors, we can make all the C-G coefficients real. As both bases are orthonormal, the transformation matrix between them must be orthogonal. This leads to [20, Section 6.2]

$$(25) \quad \sum_{j, m} \langle m_1 m_2 | jm \rangle \langle m'_1 m'_2 | jm \rangle = \delta_{m_1 m'_1} \delta_{m_2 m'_2},$$

$$(26) \quad \sum_{m_1, m_2} \langle m_1 m_2 | jm \rangle \langle m_1 m_2 | j' m' \rangle = \delta_{m, m'} \delta_{j, j'},$$

where δ_{ij} is the Kronecker delta function, and an expression of $|m_1 m_2\rangle$ in terms of $|jm\rangle$:

$$(27) \quad |m_1 m_2\rangle = \sum_{j, m} \langle m_1 m_2 | jm \rangle |jm\rangle.$$

We can also define J_{\pm} for \mathbf{J} in a way similar to how $J_{1\pm}$ was defined for \mathbf{J}_1 . Clearly $J_{\pm} = J_{1\pm} + J_{2\pm}$. We apply J_{\pm} on both sides of (24), substitute $|jm\rangle$ in terms of $|m_1m_2\rangle$, and obtain the following equation by comparing coefficients of $|m_1m_2\rangle$:

$$(28) \quad \begin{aligned} & \sqrt{(j \mp m)(j \pm m + 1)} \langle m_1m_2 | j, m \pm 1 \rangle \\ &= \sqrt{(j_1 \mp m_1 + 1)(j_1 \pm m_1)} \langle m_1 \mp 1, m_2 | j, m \rangle \\ & \quad + \sqrt{(j_2 \mp m_2 + 1)(j_2 \pm m_2)} \langle m_1, m_2 \mp 1 | j, m \rangle. \end{aligned}$$

Instead of calculating the matrix elements of $\mathbf{d}^+ \cdot \mathbf{E}^+$ in the image of $|jm\rangle$, we calculate those of a group of linear combinations of the components of \mathbf{r} . Since $\mathbf{d} = \sum_n q_n \mathbf{r}_n$, where q_k is the electric charge of a particle, our results can be generalized to \mathbf{d} with a little extra work. This is actually a special example of the famous *Wigner-Eckart theorem*¹. An elegant derivation can be found in [20] using group theory. Leaving the details to references, we start by defining

$$(29) \quad r_1 = \frac{1}{\sqrt{2}}(-ix + y), \quad r_0 = iz, \quad r_{-1} = \frac{1}{\sqrt{2}}(ix + y).$$

Let $\mathbf{L} = \hbar^{-1} \mathbf{r} \times \mathbf{p}$ be the orbital spin, and define J_{\pm} as

$$J_{\pm} = (L_x \pm i L_y).$$

We can easily show that

$$[J_+, r_{-1}] = \sqrt{2}r_0, \quad [J_+, r_0] = \sqrt{2}r_1, \quad [J_+, r_1] = 0,$$

and

$$[J_-, r_{-1}] = 0, \quad [J_-, r_0] = \sqrt{2}r_{-1}, \quad [J_-, r_1] = \sqrt{2}r_0.$$

In short,

$$(30) \quad [J_{\pm}, r_k] = \sqrt{(1 \mp k)(2 \pm k)} r_{k \pm 1}, \quad k = -1, 0, 1.$$

We notice that the above equations still work when J_{\pm} is defined from the total spin instead of only the orbital spin, since the electron spin and atomic spin commute with \mathbf{r} . A tensor whose components satisfy the above equations is called an irreducible tensor.

By multiplying (30) by $\langle j, m |$ on the left and $|j', m'\rangle$ on the right, we get

$$\langle j, m | J_{\pm} r_k | j', m' \rangle - \langle j, m | r_k J_{\pm} | j', m' \rangle = \sqrt{(1 \mp k)(2 \pm k)} \langle j, m | r_{k \pm 1} | j', m' \rangle.$$

The first term then can be further changed to

$$\langle j, m | J_{\pm} r_k | j', m' \rangle = \sqrt{(j \pm m)(j \mp m + 1)} \langle j, m \mp 1 | r_k | j', m' \rangle$$

by using $\langle j, m | J_{\pm} = (J \mp |j, m\rangle)^{\dagger}$. The second term on the left can also be changed to

$$\langle j, m | r_k J_{\pm} | j', m' \rangle = \sqrt{(j' \mp m')(j' \pm m' + 1)} \langle j, m | r_k | j', m' \pm 1 \rangle.$$

¹For the reader's information, we state the Wigner-Eckart theorem here.

THEOREM Let T_s^k be an irreducible tensor operator of rank s . Its matrix element between angular momentum eigenvectors $|\alpha jm\rangle$, where α is a collective label for all other quantum numbers independent of \mathbf{J} , $\langle \alpha jm | T_s^k | \alpha' j' m' \rangle$, can be factorized as

$$\langle \alpha jm | T_s^k | \alpha' j' m' \rangle = \langle j' m' s k | j m \rangle \langle \alpha j || T_k || \alpha' j' \rangle,$$

where $\langle \alpha j || T_k || \alpha' j' \rangle$ is independent of m, m' , and k , and is called the reduced matrix element. The double bar symbol enclosing T_k refers to an element of the reduced matrix instead of the full operator T_s^k .

The overall equation then becomes

$$(31) \quad \begin{aligned} & \sqrt{(1 \mp k)(2 \pm k)} \langle jm | r_{k \pm 1} | j', m' \rangle \\ &= \sqrt{(j \pm m)(j \mp m + 1)} \langle j, m \mp 1 | r_k | j', m' \rangle \\ & \quad - \sqrt{(j' \mp m')(j' \pm m' + 1)} \langle j, m | r_k | j', m' \pm 1 \rangle. \end{aligned}$$

We rewrite (28) by rearranging the order of the three terms and letting $j_2 = 1$, and get

$$(32) \quad \begin{aligned} & \sqrt{(1 \mp m_2)(2 \pm m_2)} \langle m_1, m_2 \pm 1 | j, m \rangle \\ &= \sqrt{(j \pm m)(j \mp m + 1)} \langle m_1, m_2 | j, m \mp 1 \rangle \\ & \quad - \sqrt{(j_1 \mp m_1)(j_1 \pm m_1 + 1)} \langle m_1 \pm 1, m_2 | j, m \rangle. \end{aligned}$$

Compare (32) with (31). Upon identifying j' and m' in (31) with j_1 and m_1 in (32), respectively, we conclude

$$(33) \quad \langle jm | r_k | j', m' \rangle = C \langle j' m' 1 k | jm \rangle,$$

where C is a constant which is a property of the physical quantity \mathbf{r} , depending on j and j' , and being independent of m' , k , or m . Note here that the value of j_2 is actually the rank of the tensor \mathbf{r} . The above equation shows that a matrix element of r_k actually has two parts. One of them covers all the geometric properties and is a C-G coefficient, and the other remains constant for all m' , k , and m .

2.3.3. *The effective Hamiltonian.* The Wigner-Eckart theorem implies that there is \mathcal{D} such that

$$(34) \quad \langle J_e m | \mathbf{e}_q \cdot \mathbf{d}^+ | J_g \mu \rangle = \mathcal{D} \langle J_g \mu 1 q | J_e m \rangle,$$

where $\langle J_g \mu 1 q | J_e m \rangle$ is a C-G coefficient and \mathcal{D} is independent of the magnetic quantum numbers m , μ , and q . Here the three vectors \mathbf{e}_q are actually \mathbf{e}_+ , \mathbf{e}_z , and \mathbf{e}_- , in order of $q = 1, 0, -1$, respectively. By changing the relative phases of e and g states, we can always make \mathcal{D} a real number. The expression can further be simplified by introducing two new operators $\hat{\mathbf{d}}^+$ and $\hat{\mathbf{d}}^-$ through

$$(35) \quad \begin{aligned} \hat{\mathbf{d}}^+ &= \frac{1}{\mathcal{D}} \mathbf{d}^+, \\ \hat{\mathbf{d}}^- &= \frac{1}{\mathcal{D}} \mathbf{d}^-, \end{aligned}$$

Then the matrix elements of $\mathbf{e}_q \cdot \hat{\mathbf{d}}^+$ will be just the Clebsch-Gordan coefficients. We can also define operators G^+ and G^- for future use:

$$(36) \quad \hbar G^\pm = \mathbf{d}^\pm \cdot \mathbf{E}^\pm(z).$$

The evolution of a general atom in the above field is described by its density operator σ . In terms of σ_{ee} , σ_{eg} , σ_{ge} , and σ_{gg} , its equations of motion, called the Bloch equations, are given by (see, e.g., [10, page 91])

$$(37) \quad \begin{aligned} \dot{\sigma}_{ee} &= -\Gamma \sigma_{ee} + i(G^+ \tilde{\sigma}_{ge} - \tilde{\sigma}_{eg} G^-), \\ \dot{\tilde{\sigma}}_{eg} &= -(\frac{\Gamma}{2} - i\delta) \tilde{\sigma}_{eg} + i(G^+ \sigma_{gg} - \sigma_{ee} G^+), \\ \dot{\sigma}_{gg} &= (\frac{d}{dt} \sigma_{gg})_{sp} + i(G^- \tilde{\sigma}_{eg} - \tilde{\sigma}_{ge} G^+), \end{aligned}$$

where $(\frac{d}{dt} \sigma_{gg})_{sp}$ describes the damping due to spontaneous emission and Γ is the natural width of the excited state which can be considered as the *relaxation time* associated with the *spontaneous emission*. Also appearing in above equations are $\tilde{\sigma}_{eg} \equiv \sigma_{eg} e^{i\omega t}$, and $\delta \equiv \omega - \omega_A$.

We now invoke the limit of low saturation and low velocity to simplify the Bloch equation (37). When the intensity of the laser is low and the velocity of the atom

is small, the evolution of σ_{gg} is much slower than that of σ_{ge} and σ_{ee} . It follows that $\tilde{\sigma}_{eg}$, $\tilde{\sigma}_{ge}$, and σ_{ee} can be replaced by algebraic expressions in terms of σ_{gg} , and are given by

$$(38) \quad \begin{aligned} \tilde{\sigma}_{eg} &= -\frac{1}{\delta+i(\Gamma/2)}G^+(z)\sigma_{gg}, \\ \tilde{\sigma}_{ge} &= -\frac{1}{\delta-i(\Gamma/2)}\sigma_{gg}G^-, \\ \sigma_{ee} &= -\frac{i}{\Gamma(\delta-i(\Gamma/2))}G^+\sigma_{gg}G^- + h.c. \end{aligned}$$

where $h.c.$ means the Hermitian conjugate.

By substituting (38) back into (37), we can obtain a closure equation for σ_{gg} :

$$(39) \quad \begin{aligned} \dot{\sigma}_{gg} &= -\frac{i}{\delta+i(\Gamma/2)}G^-G^+\sigma_{gg} + \frac{i}{\delta-i(\Gamma/2)}\sigma_{gg}G^-G^+ \\ &\quad + \frac{\Gamma}{\delta^2+\Gamma^2/4}\Sigma_{q=-1,0,1}\mathbf{e}_q^* \cdot \hat{\mathbf{d}}^- G^+\sigma_{gg}G^-\mathbf{e}_q \cdot \hat{\mathbf{d}}^+, \end{aligned}$$

where the last term describes the effect due to the spontaneous emission. The first two terms on the right-hand side of (39), denoted as $(\dot{\sigma}_{gg})_{las}$, can be rewritten as

$$(40) \quad \begin{aligned} (\dot{\sigma}_{gg})_{las} &= -i\frac{\delta}{\delta^2+(\Gamma^2/4)}[G^-(z)G^+(z), \sigma_{gg}] \\ &\quad - \frac{\Gamma/2}{\delta^2+(\Gamma^2/4)}\{G^-(z)G^+(z), \sigma_{gg}\}_+, \end{aligned}$$

where $[X, Y] = XY - YX$ is the commutator and $\{X, Y\}_+ = XY + YX$ is the anticommutator.

By defining

$$(41) \quad \begin{aligned} \hat{\Gamma}(z) &= \Gamma \frac{\Omega_1^2(z)/4}{\delta^2+(\Gamma^2/4)} = \Gamma \frac{s(z)}{2}, \\ \hat{\delta}(z) &= \delta \frac{\Omega_1^2(z)/4}{\delta^2+(\Gamma^2/4)} = \delta \frac{s(z)}{2}, \end{aligned}$$

where $s(z) = \frac{\Omega_1^2(z)/2}{\delta^2+(\Gamma^2/4)}$ and $\Omega_1(z) = -\mathcal{D}\epsilon/\hbar$, and introducing operator Λ as

$$(42) \quad \Lambda(z) = (\mathbf{e}^* \cdot \hat{\mathbf{d}}^-)(\mathbf{e} \cdot \hat{\mathbf{d}}^+) = \Lambda^+(z),$$

we obtain

$$(43) \quad \begin{aligned} \dot{\sigma}_{gg} &= -i\hat{\delta}(z)[\Lambda(z), \sigma_{gg}] - \frac{\hat{\Gamma}(z)}{2}\{\Lambda(z), \sigma_{gg}\}_+ \\ &\quad + \hat{\Gamma}(z)\Sigma_{q=-1,0,1}\mathbf{e}_q^* \cdot \hat{\mathbf{d}}^- G^+\sigma_{gg}G^-\mathbf{e}_q \cdot \hat{\mathbf{d}}^+. \end{aligned}$$

The evolution of σ_{gg} given by (43) implies an effective Hamiltonian H_{eff} for the atom with multiple sub-levels in its ground state:

$$(44) \quad H_{eff} = \hbar\hat{\delta}(z)\Lambda(z) = \frac{\hbar\delta}{\delta^2+(\Gamma^2/4)}G^-(z)G^+(z).$$

LEMMA 2.1. *Both the operators Λ and $G^-(z)G^+(z)$ are hermitian and semi-positive.*

PROOF. According to its definition,

$$(45) \quad (G^+(z))^\dagger = \left(\frac{1}{\hbar}(\mathbf{d}^+ \cdot \mathbf{E}^+z)\right)^\dagger = G^-.$$

Thus

$$(46) \quad (G^-(z)G^+(z))^\dagger = G^-(z)G^+(z).$$

Similarly,

$$(47) \quad \Lambda(z) = (\mathbf{e}^* \cdot \hat{\mathbf{d}}^-)(\mathbf{e} \cdot \hat{\mathbf{d}}^+) = \Lambda^+(z).$$

□

THEOREM 2.2. *The eigenvalues of the effective Hamiltonian H_{eff} are real. They either have the same sign as δ or are zero.*

PROOF. Since Λ is Hermitian and semi-positive, its eigenvalues are real and nonnegative. Let $|g_\alpha\rangle$ be an eigenstate of H_{eff} with eigenvalue E_α , then $|g_\alpha\rangle$ is also an eigenstate of $\Lambda(z)$ corresponding to a nonnegative eigenvalue λ_α .

Applying H_{eff} to $|g_\alpha\rangle$, we get

$$\begin{aligned} H_{eff}|g_\alpha\rangle &= E_\alpha|g_\alpha\rangle \\ &= \hbar\hat{\delta}(z)\Lambda|g_\alpha\rangle \\ &= \hbar\hat{\delta}(z)\lambda_\alpha|g_\alpha\rangle. \end{aligned} \quad (48)$$

Thus

$$E_\alpha = \hbar\hat{\delta}(z)\lambda_\alpha. \quad (49)$$

If $\lambda_\alpha > 0$ and $\hat{\delta} \neq 0$, E_α has the same sign as $\hat{\delta}$. Otherwise, $E_\alpha = 0$. Note that δ and $\hat{\delta}$ have the same sign. \square

The ac-Stark shift is also called the light shift. If λ_α are all different, the energy shifts for different sub-levels are different and the degeneracy is removed.

In the simplest case, the ground state consists of only two sub-levels, which means $J_g = 1/2$. Consider a transition $J_g = 1/2 \leftrightarrow J_e = 3/2$, with the corresponding Clebsch-Gordan coefficients being shown in Fig. 3. In this configuration, there is no absorption-emission process leading to transition between the two ground sub-levels, and the operator Λ is diagonal. The two eigenstates of H_{eff} are also eigenstates of J_z , denoted as $|g_{\pm 1/2}\rangle$. The light shift $E_{\pm 1/2}(z)$ of $|g_{\pm 1/2}\rangle$ can be calculated using

$$E_{\pm 1/2}(z) = \hbar\hat{\delta}(z)\lambda_{\pm}(z), \quad (50)$$

where λ_+ and λ_- are the diagonal elements of the operator $\Lambda(z)$.

To make the calculations simple, we take the $\text{lin} \perp \text{lin}$ configuration as an example, and the calculations for the $\text{lin}\theta\text{lin}$ configuration will be similar. By changing the phases of the light and the origin, we can write the electric field at z as (11):

$$\mathbf{E}(z, t) = \mathbf{E}^+(z)e^{-i\omega t} + \mathbf{E}^-e^{i\omega t}, \quad (51)$$

where

$$\mathbf{E}^+(z) = \frac{1}{2}\epsilon\mathbf{e} \quad (52)$$

with

$$\mathbf{e} = \cos kz\mathbf{e}_- - i\sin kz\mathbf{e}_+, \quad (53)$$

where vectors \mathbf{e}_- and \mathbf{e}_+ are defined as before.

Using (34) and the C-G coefficients as in Fig. 3, and the definition of Λ , we get

$$\begin{aligned} \lambda_+ &= \langle g_{+1/2} | \Lambda | g_{+1/2} \rangle \\ &= \langle g_{+1/2} | (\mathbf{e}^* \cdot \hat{\mathbf{d}}^-)(\mathbf{e} \cdot \hat{\mathbf{d}}^+) | g_{+1/2} \rangle \\ &= \langle g_{+1/2} | (\mathbf{e}^* \cdot \hat{\mathbf{d}}^-) \Sigma_{m=-3/2}^{3/2} | J_e m \rangle \langle J_e m | (\mathbf{e} \cdot \hat{\mathbf{d}}^+) | g_{+1/2} \rangle \\ &= \sin^2 kz + \frac{1}{3} \cos^2 kz \\ &= 1 - \frac{2}{3} \cos^2 kz. \end{aligned} \quad (54)$$

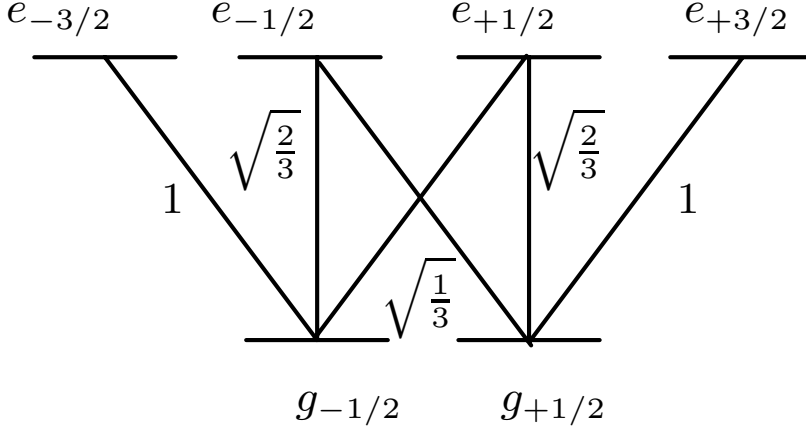


FIGURE 3. A schematic of a two-level atom and the Clebsch-Gordan coefficients for the $J_g = 1/2 \leftrightarrow J_e = 3/2$ transition.

Note that $|g_{+1/2}\rangle$ is a sublevel of the ground state with $J_g = 1/2$ and $\mu = 1/2$. Similarly, λ_- can be obtained as

$$(55) \quad \lambda_- = \cos^2 kz + \frac{1}{3} \sin^2 kz = 1 - \frac{2}{3} \sin^2 kz.$$

The light shifts $E_{+1/2}$ and $E_{-1/2}$ can then be written as

$$(56) \quad \begin{aligned} E_{+1/2} &= -\frac{3U_0}{2} + U_0 \cos^2 kz, \\ E_{-1/2} &= -\frac{3U_0}{2} + U_0 \sin^2 kz, \end{aligned}$$

where

$$(57) \quad U_0 = -\frac{2}{3} \hbar \hat{\delta} = -\frac{2}{3} \hbar \delta s_0.$$

The above results show that the degeneracy of the Zeeman sub-levels is removed in the laser field. When $\delta < 0$, both $E_{+1/2}$ and $E_{-1/2}$ are negative. When $kz = 0, \pi, 2\pi, \dots$, $E_{-1/2}$ is three times deeper than $E_{+1/2}$. When $kz = \pi/2, 3\pi/2, 5\pi/2, \dots$, the reverse situation holds.

3. Quantum computation using neutral atoms in optical lattices

3.1. One qubit gates. From Theorem 1.1, we know that the collection of all 1-qubit gates and the 2-qubit CNOT gate is universal. In addition, the following (cf. e.g., [16, p. 175]) holds for 1-qubit quantum gates.

THEOREM 3.1. *Suppose that U is a 1-qubit unitary operation. Then there exist real numbers α , β , γ , and δ such that*

$$U = e^{i\alpha} Z_\beta Y_\gamma Z_\delta,$$

where Z_β , Y_γ and Z_δ are rotation gates, see (58) below. □

For example, the Hadamard gate H can be decomposed as $H = e^{-i\frac{\pi}{2}} Y_{\pi/2} Z_\pi$. Clearly, the $x/y/z$ rotation gates provide building blocks sufficient to construct any one qubit unitary gate. These rotations are defined as follows [17]:

$$\begin{aligned}
 (58) \quad X_\theta &= e^{-i\theta\sigma_x/2} = \begin{bmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}, \\
 Y_\theta &= e^{-i\theta\sigma_y/2} = \begin{bmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix}, \\
 Z_\theta &= e^{-i\theta\sigma_z/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix},
 \end{aligned}$$

where θ is a certain angle, and σ_x , σ_y and σ_z are the Pauli matrices².

Every qubit in a quantum computer is represented by a two-level quantum system. For the neutral atom quantum computer, sub-levels of hyperfine structure manifolds of atomic ground states are stable and suitable for the purpose. Take the state with lower energy as logic state $|0\rangle$ and the state with higher energy as logic state $|1\rangle$. We can write an arbitrary state of the qubit as

$$(59) \quad |\psi\rangle = c_0|0\rangle + c_1|1\rangle.$$

where c_0 and c_1 are complex satisfying the normalized condition $|c_0|^2 + |c_1|^2 = 1$. The Hamiltonian of this two-level quantum system is analogous to that of a spin- $\frac{1}{2}$ system, given by

$$(60) \quad H_0 = \frac{\hbar\omega_{hf}}{2}(-|0\rangle\langle 0| + |1\rangle\langle 1|),$$

using the basis formed by $|0\rangle$ and $|1\rangle$, where ω_{hf} is the hyperfine structure splitting frequency between the two states (usually the F and $F+1$ states). In matrix form, H_0 can be written in terms of the Pauli matrix σ_z :

$$(61) \quad H_0 = -\frac{\hbar\omega_{hf}}{2}\sigma_z.$$

The evolution of the quantum state of the qubit is governed by the Schrödinger equation solved in matrix form as

$$\begin{aligned}
 |\psi(t)\rangle &= e^{i\omega_{hf}\sigma_z t/2}|\psi_0\rangle \\
 &= \begin{bmatrix} e^{i\omega_{hf}t/2} & 0 \\ 0 & e^{-i\omega_{hf}t/2} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} \\
 &= e^{i\omega_{hf}t/2} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\omega_{hf}t} \end{bmatrix} |\psi_0\rangle,
 \end{aligned}$$

where $|\psi(t)\rangle$ is the system state at time t , and $|\psi_0\rangle = |\psi(0)\rangle$ is the initial state. Choosing appropriate time duration t , we can obtain a z -rotation gate with an arbitrary angle.

Different from the z -rotation which makes only a phase change to the system, an x or y rotation change the state's amplitudes. This can be achieved with one microwave pulse resonant at the hyperfine frequency ω_{hf} , or two lasers with a frequency difference of ω_{hf} shining on the atom. The former causes a *Rabi rotation*, and the latter does a *Raman rotation*. Although two laser fields are involved in the Raman rotation instead of just one in the Rabi rotation, the system Hamiltonian is similar and we consider only the Rabi rotation. Assume that the microwave is

²The Pauli matrices are $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

resonant and classical, then the system Hamiltonian has two parts, the original Hamiltonian (60) plus an additional atom-laser interaction Hamiltonian:

$$(62) \quad H_I = \hbar\Omega(e^{-i(\omega_{hf}t+\alpha)}|1\rangle\langle 0| + e^{i(\omega_{hf}t+\alpha)}|0\rangle\langle 1|),$$

where Ω is the Rabi rotation frequency, and α is the sum of the phase of the complex Rabi rotation frequency with the external field. The interaction Hamiltonian is derived under the rotating wave assumption. As previously stated, the evolution of the system state is governed by the Schrödinger equation:

$$(63) \quad \begin{aligned} \frac{\partial}{\partial t}|\psi(t)\rangle &= -\frac{i}{\hbar}H|\psi(t)\rangle \\ &= -\frac{i}{\hbar}(H_0 + H_I)|\psi(t)\rangle. \end{aligned}$$

The Rabi rotation frequency, Ω , shows the coupling strength between the atom and the external field. It is also the frequency of Rabi flipping between the levels of a 2-level atom illuminated by a resonant laser beam. It is proportional to the amplitude of the external field and defined as

$$\Omega = \frac{|\mathbf{d}^+ \cdot \mathbf{E}^+|}{\hbar},$$

where \mathbf{d}^+ and \mathbf{E}^+ are defined as before. Atoms with a larger dipole moment will have a higher Rabi frequency and jump faster between the two levels. A stronger electric field has the same effect. The dot product inside the absolute value sign could be complex. In practice, its phase is separated from Ω for simplification.

THEOREM 3.2. *By changing the phase angle α and time duration, we can get an arbitrary x - or y -rotation using the Hamiltonian given in (62).*

PROOF. We first define $|\phi(t)\rangle = U_0|\psi(t)\rangle$, where

$$(64) \quad \begin{aligned} U_0 &= e^{\frac{-iH_0t}{\hbar}} \\ &= \begin{bmatrix} e^{i\omega_{hf}t/2} & 0 \\ 0 & e^{-i\omega_{hf}t/2} \end{bmatrix}. \end{aligned}$$

In other words, we put the system state in a “rotating frame”. Substituting it back to (63), we can obtain the Schrödinger equation for $|\phi\rangle$:

$$(65) \quad \frac{\partial}{\partial t}|\phi(t)\rangle = -\frac{i}{\hbar}\mathcal{H}|\phi(t)\rangle,$$

where \mathcal{H} is called the Hamiltonian in the interaction picture [18]:

$$(66) \quad \mathcal{H} = U_0^\dagger H_I U_0.$$

It can be derived by substituting U_0 and H_I into (66):

$$(67) \quad \begin{aligned} \frac{\mathcal{H}}{\hbar\Omega} &= \begin{bmatrix} e^{-i\omega_{hf}t/2} & 0 \\ 0 & e^{i\omega_{hf}t/2} \end{bmatrix} \begin{bmatrix} 0 & e^{i(\omega_{hf}t+\alpha)} \\ e^{-i(\omega_{hf}t+\alpha)} & 0 \end{bmatrix} \begin{bmatrix} e^{i\omega_{hf}t/2} & 0 \\ 0 & e^{-i\omega_{hf}t/2} \end{bmatrix} \\ &= \begin{bmatrix} 0 & e^{i\alpha} \\ e^{-i\alpha} & 0 \end{bmatrix} \\ &= \cos(\alpha)\sigma_x - \sin(\alpha)\sigma_y. \end{aligned}$$

After time duration t , the new system state is given as

$$(68) \quad |\phi(t)\rangle = e^{-i\Omega(\sigma_x \cos(\alpha) - \sigma_y \sin(\alpha))t}|\phi(0)\rangle,$$

and the evolution operator can be computed as

$$(69) \quad \begin{aligned} U_{\theta/2, \alpha} &= e^{-i\Omega(\sigma_x \cos(\alpha) - \sigma_y \sin(\alpha))t} \\ &= \begin{bmatrix} \cos(\frac{\theta}{2}) & -i \sin(\frac{\theta}{2})e^{-i\alpha} \\ -i \sin(\frac{\theta}{2})e^{i\alpha} & \cos(\frac{\theta}{2}) \end{bmatrix}, \end{aligned}$$

where $\theta = 2\Omega t$. This is a 1-qubit rotation operator, also called a Rabi rotation gate. When $\alpha = \pi/2$,

$$(70) \quad \begin{aligned} U_{\theta/2, \pi/2} &= \begin{bmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix} \\ &= Y_{\theta}, \end{aligned}$$

we have achieved a y -rotation operator in the rotating frame. An x -rotation gate in the rotating frame can be obtained similarly. The x - and y -rotation gates for state $|\psi\rangle$ can be obtained by using two additional z -rotation gates. □

3.2. Using induced dipole-dipole interaction to entangle two neutral atom qubits. Alkali atoms are commonly used for neutral atom qubits in quantum computation. These atoms include but are not limited to Na, Rb, and their isotopes. Quantum information can be encoded in the hyperfine structures of the atom, normally in the $S_{1/2}$ ground states. The energy between the two levels, or the hyperfine splitting, is in the order of GHz. Thus, microwaves can be used to induce Rabi rotations.

There are various methods to trap atoms in space, such as *optical lattices*, *laser traps*, and *magnetic microtraps* ([14]). As mentioned before, an optical lattice consists of three pairs of counter-propagating lasers along the x , y and z directions, respectively. The frequency of the lasers is far off resonance from the atom, and the two laser beams in the z directions take a linθlin configuration. (See Section 2 for more details.) Atoms trapped in such an optical lattice are separated into two groups, whose energy shift is dominated by either the σ_+ or σ_- standing wave of the lattice. These two “species” of atoms form alternate layers along the z axis. Atoms along a line parallel to the z -axis form a “tube”. Each “tube” has a collection of atoms and can be treated as a register. With fixed potential on the x and y directions, the atoms will not move in the x - y plane. However, neighboring atoms in a register (or “tube”) can be moved together or apart by changing the polarization angle between the two laser beams along the z axis. Another laser, called “catalysis laser”, can be used to induce selective dipole-dipole interaction depending on the internal state of the two atoms when it is applied to the site where it is needed.

A careful choice of the hyperfine manifold is made for the quantum logic basis. In the proposal by Brennen, et al., ([2, 3]) the logic, or computational, basis, is defined as

$$(71) \quad \begin{aligned} |1\rangle_{\pm} &= |F_{\uparrow}, M_F = \pm 1\rangle \otimes |\psi_{1\pm}\rangle_{ext}, \\ |0\rangle_{\pm} &= |F_{\downarrow}, M_F = \mp 1\rangle \otimes |\psi_{0\pm}\rangle_{ext}, \end{aligned}$$

where $+$ and $-$ are used to denote the ‘ $+$ ’ and ‘ $-$ ’ species of atoms, respectively. State $|\psi_{1\pm, 0\pm}\rangle_{ext}$ is the center of mass motion state of the atom in the potential well, also called the external state, and can be set to the ground state with $n = 0$. Opposite to the external state, the internal states are the two hyperfine levels associated with the ground state $S_{1/2}$, where $F_{\uparrow, \downarrow} = I \pm \frac{1}{2}$ is the total angular momentum, and

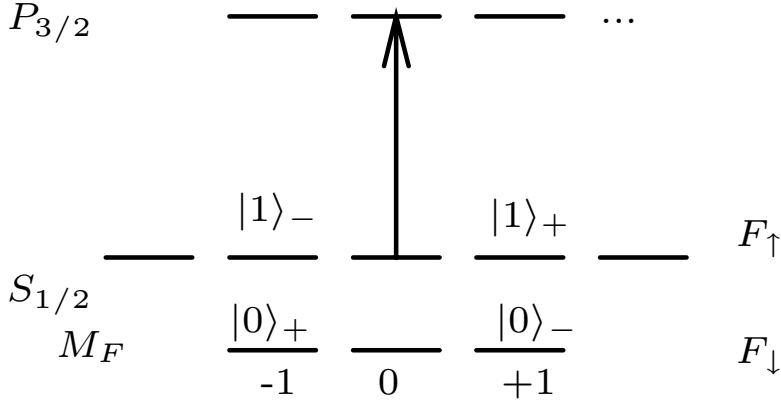


FIGURE 4. A schematic of the energy levels used to represent the logical basis $|0\rangle$ and $|1\rangle$ (not in scale). The atom used has nuclear spin $3/2$ ($I = 3/2$). Also included is the $P_{3/2}$ level which is used in the controlled phase gate.

M_F is its projection. See Fig. 4. This design has several advantages. First, phase change due to the fluctuation of the ambient magnetic field is minimized. Second, the entanglement only has an effect on the atom's angular momentum state, and will not excite the atom into higher levels out of the logic space.

The *induced dipole-dipole interaction* is utilized in this proposal to entangle two neighboring atoms. It depends on both the internal and external states. The internal state determines the nature of the interaction. On the other hand, the external state, which is the mode of center-of-mass motion, defines the probability distribution of the relative position of the two atoms. Consider two alkali atoms in a potential well with center of mass positions \mathbf{r}_1 and \mathbf{r}_2 , interacting with a classical monochromatic catalysis field. The effective Hamiltonian has two parts ([3, 12]):

$$(72) \quad H = H_{AL} + H_{dd},$$

where H_{AL} and H_{dd} are the atom-laser interaction Hamiltonian and the dipole-dipole interaction Hamiltonian, respectively. In terms of the dipole raising operator D^\dagger , which is associated with the absorption of a photon, these two terms can be written as

$$(73) \quad \begin{aligned} H_{AL} &= -\hbar(\Delta + i\frac{\Gamma}{2})(D_1^\dagger \cdot D_1 + D_2^\dagger \cdot D_2) \\ &\quad - \frac{\hbar\Omega}{2}(D_1^\dagger \cdot \mathbf{e}_L(\mathbf{r}_1) + D_2^\dagger \cdot \mathbf{e}_L(\mathbf{r}_2) + h.c.), \\ H_{dd} &= V_{dd} - i\frac{\hbar\Gamma_{dd}}{2} = -\frac{\hbar\Gamma}{2}(D_2^\dagger \cdot \overleftrightarrow{\mathbf{T}}(k_L r) \cdot D_1 + D_1^\dagger \cdot \overleftrightarrow{\mathbf{T}}(k_L r) \cdot D_2), \end{aligned}$$

where the tensor $\overleftrightarrow{\mathbf{T}}$ describes the strength of the interaction between the two atoms at distance r , \mathbf{e}_L is the polarization vector of the laser field, and V_{dd} is the dipole-dipole energy level shift. Here the anti-Hermitian part, $i\Gamma_{dd}$, i.e., $(i\Gamma_{dd})^\dagger = -i\Gamma_{dd}$, determines the spontaneous emission process.

Assume that the quantum system is contained in the finite-dimensional space spanned by the logic basis $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$, where $|00\rangle = |0\rangle_+ \otimes |0\rangle_-$, $|01\rangle = |0\rangle_+ \otimes |1\rangle_-$, $|10\rangle = |1\rangle_+ \otimes |0\rangle_-$, and $|11\rangle = |1\rangle_+ \otimes |1\rangle_-$, the above Hamiltonian can be written in matrix form. Computation for the elements is tedious [3], and we

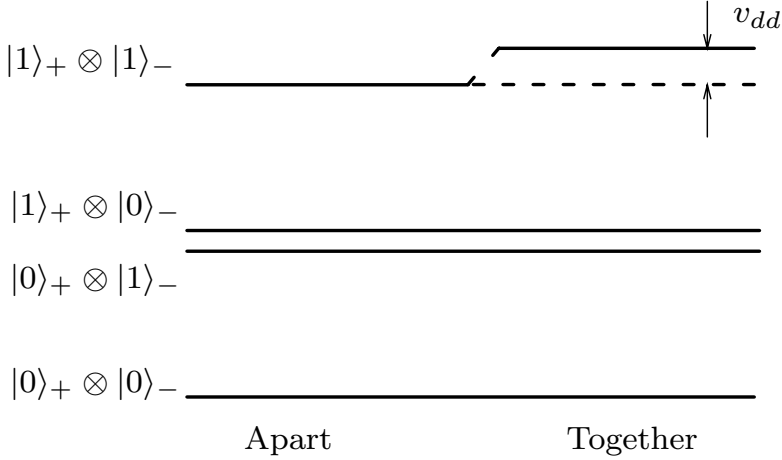


FIGURE 5. A schematic of the energy shifting for a CPHASE gate (not in scale). Only the state $|11\rangle$ obtains an obvious shifting, v_{dd} , when the atoms are moved together and is illuminated by the catalysis field.

will only discuss the setting for a controlled phase gate (CPHASE) design. If the catalysis field is tuned near the $|S_{1/2}, F_{\uparrow}\rangle \rightarrow |P_{3/2}\rangle$ resonance with small detuning compared with the ground state hyperfine splitting, dipole is excited for an atom only when the atom is in the $|F_{\uparrow}\rangle$ state. Thus, the dipole-dipole interaction is strong only when both atoms are in the $|F_{\uparrow}\rangle$ state (logic state $|1\rangle$). See Fig. 5. Otherwise, it is negligible. The induced dipole-dipole interaction only causes an energy shift to state $|11\rangle$, denoted by v_{dd} . The elements of V_{dd} , including both diagonal and off-diagonal ones, are all zero except $\langle 11|V_{dd}|11\rangle$. Written in the matrix form in terms of the basis $\{|00\rangle, |01\rangle, |10\rangle, \text{ and } |11\rangle\}$, both H_{AL} and V_{dd} are diagonal and V_{dd} has a simple form:

$$(74) \quad V_{dd} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & v_{dd} \end{bmatrix}.$$

Since the evolution contributed by H_{AL} can always be compensated by additional 1-qubit operations before and/or after the entanglement, a controlled phase gate (CPHASE) can be obtained if the interaction lasts for time duration t :

$$(75) \quad U(\theta) = e^{-iV_{dd}t/\hbar} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{-i\theta} \end{bmatrix},$$

where $\theta = \frac{v_{dd}t}{\hbar}$. When $\theta = \pi$,

$$(76) \quad U(\pi) = e^{-iV_{dd}t/\hbar} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}.$$

A controlled NOT gate can be obtained by combining $U(\pi)$ with several 1-qubit operations.

3.3. Using cold atom collisions to entangle two neutral atoms. Neutral atoms can also be entangled using *controlled cold atom collisions* [15], where the S-wave dominates the process. We here assume that the collisions are elastic. When the time duration of the interaction is chosen carefully, the collision results in a selective phase change only for one special state of a two-atom system, and entanglement is achieved. Consider two atoms trapped in two neighboring potential wells formed in the optical lattice. Two strategies are available to achieve this selective interaction:

- (i) one can move the potential wells depending on the states of the atoms;
- (ii) one can also switch the potential selectively so that the atoms can tunnel through the well and collide with each other only when both atoms are in $|0\rangle$ state.

Here, we will give more details for (i) and leave (ii) to a separate article.

As in the previous subsection, we still consider alkali atoms with nuclear spin- $\frac{3}{2}$ trapped in an optical lattice. The three dimensional lattice consists of standing waves along the x , y and z axis. The standing wave along the z axis takes the $\text{lin}\theta\text{lin}$ configuration as discussed in Subsection 2.1, so that we can move the atoms along the z axis. The laser is blue-tuned between the $P_{1/2}$ and $P_{3/2}$ levels, see Fig. 6. In this configuration, the dynamic polarization of the $S_{1/2}$ fine structure with $m_s = 1/2$ due to laser polarization σ_- , α_{-+} , vanishes, so does that of the $S_{1/2}$ fine structure with $m_s = -1/2$ due to laser polarization σ_+ , α_{+-} ; however, the dynamic polarization of $S_{1/2}$ fine structure with $m_s = 1/2$ due to laser polarization σ_+ , α_{++} , does not vanish, and is equal to α_{--} , that of the $S_{1/2}$ fine structure with $m_s = -1/2$ due to laser polarization σ_- . As explained in the preceding section, atoms with $m_s = +1/2$ and $m_s = -1/2$ experience different potentials in a $\text{lin} \perp \text{lin}$ configured optical lattice. After removing the common terms in (56) and choosing the proper origin, we can write the potentials for atoms with $m_s = +1/2$ and $m_s = -1/2$ as

$$(77) \quad \begin{aligned} V_{m_s=1/2}(z, \theta) &= \alpha\epsilon^2 \sin^2(kz + \theta/2), \\ V_{m_s=-1/2}(z, \theta) &= \alpha\epsilon^2 \sin^2(kz - \theta/2), \end{aligned}$$

respectively, where θ is the angle between the polarization directions of the two counter propagating laser beams along the z axis, $\alpha = \alpha_{++} = \alpha_{--}$, and k is the angular wave number. When $\theta = 0$ or $\theta = \pi$, polarizations along the z -axis are linear everywhere, and $V_{m_s=1/2}(z, \theta) = V_{m_s=-1/2}(z, \theta)$. Otherwise, $V_{m_s=1/2}(z, \theta) \neq V_{m_s=-1/2}(z, \theta)$, and the minimum points of $V_{m_s=1/2}(z, \theta)$ and $V_{m_s=-1/2}(z, \theta)$ do not coincide and are distributed alternatively along the z -axis.

The binary quantum states assigned to represent the logic states are two $S_{1/2}$ hyperfine structure states:

$$(78) \quad \begin{aligned} |0\rangle &= |F_{\downarrow}, m_f = 1\rangle, \\ |1\rangle &= |F_{\uparrow}, m_f = 2\rangle, \end{aligned}$$

and the external states (due to the center-of-mass motion) are initialized to the ground state. These two states are stable in collision due to the conservation of angular momentum. Their potentials along the z axis can be derived in terms of

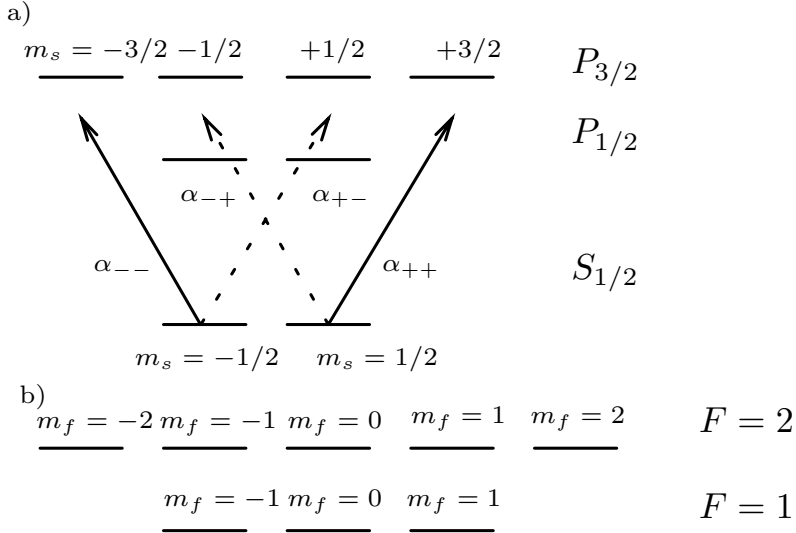


FIGURE 6. A schematic of the energy levels and laser configuration. (a) fine structure and laser configuration, (b) superfine structure of $S_{1/2}$.

the C-G coefficients. Since

$$(79) \quad \begin{aligned} |0\rangle &= -\frac{1}{2}|J = \frac{1}{2}, m_s = \frac{1}{2}, m_I = \frac{1}{2}\rangle + \frac{\sqrt{3}}{2}|J = \frac{1}{2}, m_s = -\frac{1}{2}, m_I = \frac{3}{2}\rangle, \\ |1\rangle &= |J = \frac{1}{2}, m_s = \frac{1}{2}, m_I = \frac{3}{2}\rangle, \end{aligned}$$

the potentials (for the Hamiltonian) of the two states can be given as combinations of $V_{m_s=1/2}$ and $V_{m_s=-1/2}$:

$$(80) \quad \begin{aligned} V^0(z, \theta) &= (V_{m_s=1/2}(z, \theta) + 3V_{m_s=-1/2}(z, \theta))/4, \\ V^1(z, \theta) &= V_{m_s=1/2}(z, \theta). \end{aligned}$$

If θ is set to 0 or π , V^0 and V^1 are the same. When θ changes from 0 to π , or from π to 0, V^0 and V^1 move to opposite directions and overlap. While the potential moves, the corresponding atoms move with it along the z axis back and forth depending on their internal state. Two neighboring atoms will be moved into one potential well only when the left atom is in state $|0\rangle$ and the right atom is in state $|1\rangle$. We assume that the change is adiabatic, and that the atoms will not be excited to higher external levels. Spontaneous emissions by atoms from the higher level may cause leakage or decoherence. Another source of decoherence is inelastic collisions.

The Hamiltonian for such two trapped atoms can be written as

$$(81) \quad \begin{aligned} H^{\beta_1\beta_2} &= \sum_{i=1,2} \left[\frac{p_i^2}{2m} + V^{\beta_i}(\mathbf{r}_i, t) \right] + u^{\beta_1\beta_2}(\mathbf{r}_1 - \mathbf{r}_2), \\ u^{\beta_1\beta_2}(\mathbf{r}_1 - \mathbf{r}_2) &= \frac{4\pi a_s^{\beta_1\beta_2} \hbar^2}{m} \delta^3(\mathbf{r}_1 - \mathbf{r}_2), \end{aligned}$$

where $\mathbf{r}_{1,2}$ are the positions of the two atoms, respectively, while $u^{\beta_1\beta_2}$ is the interaction potential, and V^{β_i} is the potential function of atom i , which depends on its internal state. We use i to tell one atom apart from another, and β_i to denote the internal state of atom i . Assume that the energy shift caused by collisions

is small so that we can use perturbation theory. Under this assumption, the interaction Hamiltonian is still diagonal using basis $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, where $|\beta_1\beta_2\rangle$ represents state $|\beta_1\rangle_1|\beta_2\rangle_2$, $\beta_{1,2} = 0, 1$. Thus the evolution results in only a phase change. This phase change consists of two parts: the kinetic phase due to the kinetic energy and the interaction phase due to the collision. Both depend on the atoms' internal state.

The kinetic phase is accumulated while the atom moves with the potential well it is in. Assume that the atom has internal state $|\beta\rangle$ and its external state is in the ground state $|\psi_0\rangle$ of a potential well $V(\mathbf{r} - \mathbf{r}^\beta(t))$. If the potential moves slow enough, the mass center of the atom will follow the trajectory of the minimum point of the potential well, $\mathbf{r}^\beta(t)$, which depends on the internal state β . The kinetic phase change accumulated from $-\tau$ to τ is given by

$$(82) \quad \phi^\beta = \frac{m}{2\hbar} \int_{-\tau}^{\tau} dt (\dot{\mathbf{r}}^\beta)^2.$$

We consider only the interaction phase when the system is originally in state $|01\rangle$, because this is the only case that collision between two atoms occurs, otherwise the two atoms are far apart. Using perturbation theory, the time dependent interaction energy can be derived as

$$(83) \quad \Delta E^{01}(t) = \frac{4\pi a_s^{01} \hbar^2}{m} \int d\mathbf{r} |\psi_1^0(\mathbf{r}, t) \psi_2^1(\mathbf{r}, t)|^2,$$

where ψ_1^0 and ψ_2^1 are the normalized one-particle wave function of atom 1 and 2 with internal state $|0\rangle$ and $|1\rangle$, respectively. The interaction phase accumulated from time $-\tau$ and τ due to the interaction is then given by the integral

$$(84) \quad \phi^{01} = \frac{1}{\hbar} \int_{-\tau}^{\tau} \Delta E^{01}(t) dt.$$

Assume that the potential wells begin to move at time $-\tau$ and resume their original positions at time τ , evolutions for the four basis are then determined as follows:

$$(85) \quad \begin{aligned} |00\rangle &\rightarrow e^{-i2\phi^0} |00\rangle, \\ |01\rangle &\rightarrow e^{-i(\phi^0 + \phi^1 + \phi^{01})} |01\rangle, \\ |10\rangle &\rightarrow e^{-i(\phi^0 + \phi^1)} |10\rangle, \\ |11\rangle &\rightarrow e^{-i2\phi^1} |11\rangle. \end{aligned}$$

After being put in matrix form, the above evolution can be given as a product of three matrices:

$$(86) \quad \begin{aligned} U &= \begin{bmatrix} e^{-i2\phi^0} & & & \\ & e^{-i(\phi^0 + \phi^1 + \phi^{01})} & & \\ & & e^{-i(\phi^0 + \phi^1)} & \\ & & & e^{-i(2\phi^1)} \end{bmatrix} \\ &= Z_{\phi^0 - \phi^1}^1 Z_{\phi^0 - \phi^1}^2 \begin{bmatrix} 1 & & & \\ & e^{-i\phi^{01}} & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \end{aligned}$$

where $Z_{\phi^0 - \phi^1}^i$ is a z -rotation gate for qubit i . Since these 1-qubit gates can always be compensated, we obtain an entangled 2-qubit gate by combining the above matrix

with additional 1-qubit operations:

$$(87) \quad U_2 = \begin{bmatrix} 1 & & & \\ & e^{-i\phi_{01}} & & \\ & & 1 & \\ & & & 1 \end{bmatrix}.$$

THEOREM 3.3. *A controlled phase shift gate can be obtained by using U_2 and two additional NOT gate on the qubit 2:*

$$(88) \quad CPHASE = U_{not}^2 \cdot U_2 \cdot U_{not}^2,$$

where U_{not}^2 is a NOT gate on qubit 2 and can be written in matrix form:

$$(89) \quad U_{not}^2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

PROOF. Straightforward substitution and verification. \square

Acknowledgments

We thank the reviewer for helpful suggestions and for pointing out several additional references.

References

- [1] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* **52**(1995), 3457–3467.
- [2] G.K. Brennen, C.M. Caves, P.S. Jessen, and I.H. Deutsch, Quantum logic gates in optical lattices, *Phys. Rev. Lett.* **82**(1999), 1060–1063.
- [3] G.K. Brennen, I.H. Deutsch, and P.S. Jessen, Entangling dipole-dipole interaction for quantum logic with neutral atoms, *Phys. Rev. A* **61**(2000), 062309.
- [4] H.J. Briegel, T. Calarco, D. Jaksch, J.I. Cirac, and P. Zoller, Quantum computing with neutral atoms, *J. Mod. Opt.* **47**(2000), 415 – 451.
- [5] J.-L. Brylinski and R. Brylinski, Universal quantum gates, in *Mathematics of Quantum Computation*, R. Brylinski and G. Chen, (eds.), Chapman & Hall/CRC, Boca Raton, Florida, 2002, 101–116.
- [6] T. Calarco, E.A. Hinds, D. Jaksch, J. Schmiedmayer, J.I. Cirac, and P. Zoller, Quantum gates with neutral atoms: controlling collisional interactions in time-dependent traps, *Phys. Rev. A* **61** (2000), 022304.
- [7] G. Chen, D.A. Church, B.-G. Englert, C. Henkel, B. Rohwedder, M.O. Scully, and M.S. Zubairy, *Quantum Computing Devices, Principles, Designs and Analysis*, Chapman & Hall/CRC, Boca Raton, Florida, 2006.
- [8] G. De Chiara, et al., Optimal control of atom transport for quantum gates in optical lattice, *Phys. Rev. A* **77** (2008), 052333.
- [9] I.L. Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd, Experimental realization of a quantum algorithm, *Nature* **393** (1998), 143–146.
- [10] C. Cohen-Tannoudji, Atomic motion in laser light, in Les Houches, Session LIII, *Fundamental Systems in Quantum Optics*, edited by J. Dailibard, J. Raimond, and J. Zinn-Justin (Elsevier Science Publisher B.V., 1990), 1–164.
- [11] D.G. Cory, A.F. Fahmy, and T.F. Havel, Ensemble quantum computing by NMR spectroscopy, *Proc. Natl. Acad. Sci. USA*, **94** (1997), 1634–1639.
- [12] I.H. Deutsch and G.K. Brennen, Quantum computing with neutral atoms in an optical lattice, in *Scalable Quantum Computer*, edited by S.L. Braunstein and H.K. Lo (Wiley-VCH, 2001), 155–173.

- [13] D.P. DiVincenzo, Two-bit quantum gates are universal for quantum computation, *Phys. Rev. A* **51**(1995), 1015–1022.
- [14] W. Hansel, J. Reichel, P. Hommelhoff, and T.W. Hansch, Trapped-atom interferometer in magnetic microtrap, *Phys. Rev. A* **64**(2001), 063607.
- [15] D. Jaksch, H.J. Briegel, J.I. Cirac, C.W. Gardiner, and P. Zoller, Entanglement of atoms via cold controlled collisions, *Phys. Rev. Lett* **82**(1999), 1975 – 1978.
- [16] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, U.K., 2000.
- [17] J. Normand, *A Lie Group: Rotations in Quantum Mechanics*, North-Holland, New York, 1980.
- [18] M. Scully and M.S. Zubairy, *Quantum Optics*, Cambridge University Press, Cambridge, U.K., 1997.
- [19] J. Sebby-Strabley, M. Anderlini, P.S. Jessen, and J.V. Porto, Lattice of double wells for manipulating pairs of cold atoms, *Phys. Rev. A* **73** (2006), 033605.
- [20] G. Trigg, *Quantum Mechanics*, D. Van Nostrand Company, Princeton, New Jersey, 1964.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HOUSTON, HOUSTON, TX 77204-3476
E-mail address: `zgzhang@math.uh.edu`

DEPARTMENT OF MATHEMATICS AND INSTITUTE FOR QUANTUM STUDIES, TEXAS A&M UNIVERSITY, COLLEGE STATION, TX 77843-3368
E-mail address: `gchen@math.tamu.edu`

Charge Renormalization, Apéry's Number, and the Trefoil Knot

Howard E. Brandt

ABSTRACT. In the context of the charge renormalization constant of quantum electrodynamics, I explore, by example, the connections between Feynman graphs, irrational or transcendental numbers, and knots. I first review the calculation in Feynman gauge of the divergent part of the inverse charge renormalization constant to sixth order in the bare charge of the electron. I identify those vacuum polarization graphs which yield Apéry's number, and describe the gauge invariant vanishing of the overall coefficient of this irrational number appearing in the sixth-order calculation. I also elucidate the mapping of vacuum polarization graphs with crossed photon propagators onto the trefoil knot.

1. INTRODUCTION

Kreimer, Broadhurst, and collaborators have in recent years explored intriguing connections between quantum field theory, number theory, and low-dimensional topology [1]. In particular, Kreimer discovered a combinatorial Hopf algebraic structure of renormalized quantum field theory, in which renormalization corresponds to the calculation of an antipode in a Hopf algebra [2]. Kreimer also explored correspondences between divergent Feynman graphs, transcendental numbers, and knots [1]. The latter is the subject of present work. In the context of the charge renormalization constant of quantum electrodynamics, I explore, by example, the connections between Feynman graphs, irrational or transcendental numbers, and knots. I review the calculation in Feynman gauge of the divergent part of the inverse charge renormalization constant in fourth and sixth order in the bare charge of the electron. I identify those vacuum polarization graphs which yield Apéry's number [3], [4], and describe the gauge invariant vanishing of the overall coefficient

2000 *Mathematics Subject Classification.* Primary 81V10, 81T18, 76F30, 37F25, 83C47, 11J82, 11J72, 57M25; Secondary 81Q30, 81T15, 11J81, 11A99, 11M99, 40A10, 32S99, 11S40.

Key words and phrases. quantum electrodynamics, charge renormalization, number theory, transcendental numbers, irrational numbers, Apéry's number, Riemann zeta function, link theory, trefoil knot, knot theory.

This work was supported by the U.S. Army Research Laboratory. The author wishes to thank Kazem Mahdavi for the invitation to present this paper at the *Conference on Representation Theory, Quantum Field Theory, Category Theory, Mathematical Physics and Quantum Information Theory*, 20-23 September 2007, at the University of Texas at Tyler.

of this irrational number appearing in the sixth-order calculation. Kreimer's mapping and also a new heuristic mapping onto links and knots of Feynman diagrams in quantum electrodynamics at infinitesimal distances are elaborated. The new model map based on physical heuristics is formulated by treating the asymptotic photon propagator as composite electron and positron propagators, and exploiting Feynman's picture of positrons as electrons moving backward in time. In particular, I elucidate the mapping of the divergent part of vacuum polarization graphs with two crossed photon propagators onto the trefoil knot.

2. CHARGE RENORMALIZATION

Intuitively, charge renormalization arises as follows. Imagine the bare charge e_0 of the electron in vacuum. The electron polarizes the vacuum, surrounding itself by a neutral cloud of electrons and positrons. Some of these, having a net charge δe , are repelled to infinity, leaving a net charge, $-\delta e$ in the part of the cloud bound to the bare test particle, within a distance of the order of the Compton wavelength of the electron, \hbar/mc . Thus the observed charge e is the renormalized charge,

$$(2.1) \quad e = e_0 - \delta e.$$

Historically, the charge renormalization constant is taken to be

$$(2.2) \quad Z_3^{1/2} = \frac{e}{e_0} = 1 - \frac{\delta e}{e_0}.$$

Mathematically, Z_3 is defined to be the residue at the pole of the unrenormalized photon propagator $D_{\mu\nu}(k)$ [5]. Thus the Lehman spectral form for $D_{\mu\nu}(k)$ is [6]

$$(2.3) \quad D_{\mu\nu}(k) = \left(g_{\mu\nu} - \frac{k_\mu k_\nu}{k^2} \right) D(k^2),$$

where k_μ is the photon wave vector (four-momentum), $g_{\mu\nu}$ is the Minkowski metric of spacetime,

$$(2.4) \quad D(k^2) = \frac{Z_3}{k^2 + i\epsilon} + \int_0^\infty d\mu^2 \frac{\sigma(\mu^2)}{k^2 - \mu^2 + i\epsilon},$$

$\sigma(\mu^2)$ is a spectral function, and ϵ is an infinitesimal. Any amplitude in the theory can be written in perturbation theory as the sum of Feynman graphs composed of connected Fermion and photon propagators. The photon line (propagator) always connects to one or two electron and/or positron lines. Using the Feynman rules, the contribution to the amplitude has the form

$$(2.5) \quad A = \dots e_0 \gamma^\mu \dots e_0 \gamma^\nu D_{\mu\nu}(q) \dots,$$

where the dots denote the integrals, traces, and other propagators occurring in the graph. Here γ^μ is a Dirac gamma matrix. The experimental charge e is determined by the interaction between the electrons and/or positrons at large distances in accord with Coulomb's law. This corresponds to small four-momentum q . Consider then the limit of A as $q^2 \rightarrow 0$, using Eqs. (2.4) and (2.5):

$$(2.6) \quad \lim_{q^2 \rightarrow 0} A = \dots \left(e_0 Z_3^{1/2} \right) \gamma^\mu \dots \left(e_0 Z_3^{1/2} \right) \gamma_\mu \frac{1}{q^2} \dots = \dots e \gamma^\mu \dots e \gamma_\mu \frac{1}{q^2} \dots$$

The observed charge is therefore taken to be

$$(2.7) \quad e = e_0 Z_3^{1/2}.$$

In the following, a general expression is obtained for the divergent part of Z_3^{-1} , expressed in terms of the vacuum polarization tensor. Since Z_3 is defined to be the residue at the pole of the factor $D(k^2)$ of the unrenormalized photon propagator at $k^2 = 0$, one has

$$(2.8) \quad Z_3 = \left(\frac{e}{e_0} \right)^2 = \lim_{k^2 \rightarrow 0} k^2 D(k^2).$$

It should be said in passing that there are three divergences in quantum electrodynamics: Z_1 , the electron-photon interaction vertex; Z_2 , the electron self energy, and Z_3^{-1} , the vacuum polarization. By the Ward identity, $Z_1 = Z_2$ [5]. From the general theory of quantum electrodynamics it is known that the function $D_{\mu\nu}(k)$ obeys the following equation [5]:

$$(2.9) \quad D_{\mu\nu}(k) = D_{\mu\nu}^{(0)}(k) - D_{\mu\lambda}^{(0)}(k) \Pi_{\lambda\sigma}(k) D_{\sigma\nu}(k).$$

Here $D_{\mu\nu}^{(0)}(k)$ is the free photon propagator, and $\Pi_{\lambda\sigma}(k)$ is the vacuum polarization tensor. In the Feynman gauge $D_{\mu\nu}^{(0)}(k)$ is given by

$$(2.10) \quad D_{\mu\nu}^{(0)}(k) = \frac{g_{\mu\nu}}{k^2}.$$

From the functional equations for the Green's functions, it is known that [5]

$$(2.11) \quad \Pi_{\mu\nu}(k) = 4\pi i \alpha_0 \text{Tr} \gamma_\mu \int \frac{d^4 p}{(2\pi)^4} S \left(p + \frac{k}{2} \right) \Gamma_\nu \left(p + \frac{k}{2}, p - \frac{k}{2} \right) S \left(p - \frac{k}{2} \right).$$

Here, α_0 is the bare fine structure constant,

$$(2.12) \quad \alpha_0 \equiv \frac{e_0^2}{4\pi},$$

Tr denotes the trace, and $S(p)$ is the unrenormalized electron Green's function. Its zero-order perturbation theory value is given by

$$(2.13) \quad S^{(0)}(p) = (i\gamma p + m)^{-1}$$

for electron momentum p and physical mass m . Also, $\Gamma^\mu(p, p')$ is the unrenormalized vertex function. To lowest order it is

$$(2.14) \quad \Gamma_\mu(p, p') = \gamma_\mu.$$

The Feynman rules for Feynman diagrams in the Feynman gauge are as follows [7]:

- electron or positron line: $(i\gamma p + m)^{-1}$,
- photon line: $g_{\mu\nu}/k^2$,
- vertex: γ_μ ,
- pair of vertices: ie_0^2 ,
- loop: $(2\pi)^{-4} d^4 k$.

The vacuum polarization tensor $\Pi_{\mu\nu}$, diagrammatically expanded to sixth order in the bare charge e_0 , is

$$\Pi_{\mu\nu} = \begin{array}{c} \text{[Diagram 1]} + \text{[Diagram 2]} + \text{[Diagram 3]} + \text{[Diagram 4]} \\ + \text{[Diagram 5]} + \text{[Diagram 6]} + \text{[Diagram 7]} + \text{[Diagram 8]} \\ + \text{[Diagram 9]} + \text{[Diagram 10]} + \text{[Diagram 11]} + \text{[Diagram 12]} \\ + \text{[Diagram 13]} + \text{[Diagram 14]} + \text{[Diagram 15]} + \text{[Diagram 16]} \\ + \text{[Diagram 17]} + \text{[Diagram 18]} \\ + \text{[Diagram 19]} + \text{[Diagram 20]} + \text{[Diagram 21]} + \text{[Diagram 22]} + \dots \end{array} \quad (2.15)$$

Here, the first graph represents the second-order term; the second, third and fourth graphs represent the fourth-order terms; and the remaining graphs represent the sixth-order terms. All possible topologies up to and including sixth order are represented by these twenty-two graphs. The eighth, twelfth, and sixteenth graphs contain photon self-energy insertions. The latter three graphs are to be dropped under the assumption that $D(k^2) \rightarrow 1/k^2$ sufficiently rapidly as $k^2 \rightarrow \infty$ for space-like k [8], (Otherwise, they would produce higher order logarithmic divergences.) This is in accord with the Johnson-Baker-Willey program of finite quantum electrodynamics [9], in which if $Z_3 \neq 0$, then Z_1 and Z_2 are finite if the bare electron mass $m_0 = 0$, and in a suitable gauge,

$$(2.16) \quad Z_3^{-1} = f(\alpha_0) \ln \left(\frac{M^2}{m^2} \right),$$

where m is the physical rest mass of the electron, M is an infinite cutoff mass, and for sufficiently small ϵ ,

$$(2.17) \quad f(\alpha_0) = 0, \quad f'(\alpha_0) = -\frac{|\epsilon|}{\alpha_0} < 0.$$

It can be shown that the divergent part of Z_3^{-1} is given by [7], [10]

$$(2.18) \quad \begin{aligned} (Z_3^{-1})_{\text{div}} &= -\frac{p^4 \alpha_0}{48 \cdot 2\pi} \ln \frac{M^2}{m^2} \\ \text{Tr} \frac{\partial^2}{\partial k_\alpha \partial k^\alpha} \gamma_\mu S \left(p + \frac{k}{2} \right) \Gamma^\mu \left(p + \frac{k}{2}, p - \frac{k}{2} \right) S \left(p - \frac{k}{2} \right) &\Big|_{k=0, m=0}. \end{aligned}$$

Note that this asymptotic expression is to be evaluated for wave vector $k = 0$ and physical mass $m = 0$. In evaluating the loop integral, a Wick rotation is exploited so that all integrals are over Euclidean four-momentum variables, and

$$(2.19) \quad \int d^4 p = \frac{i}{2} \int d\Omega_p p^2 dp^2, \quad \int d\Omega_p = 2\pi^2,$$

in which $d\Omega_p$ is the four-dimensional Euclidean angular integration measure.

3. JOST-LUTTINGER TERM

The fourth-order term in Eq. (2.18) can be shown to be given by [11], [7], [10]:

$$(3.1) \quad (Z_3^{-1})_{\text{div}}^{(4)} = -\frac{p^4}{48} \frac{\alpha_0}{2\pi} \ln \frac{M^2}{m^2} T,$$

in which the Feynman diagrammatic representation of T is:

$$(3.2) \quad T/2 = \text{[Four Feynman diagrams showing electron loops with photon insertions]} + \dots$$

Here a single slash represents $\partial/\partial k_\alpha$ and a double slash represents $\partial^2/\partial k_\alpha \partial k^\alpha$, the momentum k is always rooted through Fermion lines, and $m = 0$ in the Fermion (electron or positron) propagators. Using the Feynman rules to evaluate the diagrams in Feynman gauge, one obtains [10]:

$$(3.3) \quad T = \text{Tr} \int \frac{d^4 q}{(2\pi)^4} \frac{ie_0^2 (\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha) \gamma_\beta (\gamma_\mu \gamma (p-q) \gamma_\alpha - \gamma_\alpha \gamma (p-q) \gamma_\mu) \gamma_\beta}{2p^4 i^2 q^2 2(p-q)^4 i^2}.$$

Using the algebra of the Dirac gamma matrices (Appendix 1), Wick rotating the four-momenta so they are Euclidean vectors, expanding the momentum-difference denominator in Chebyshev polynomials (Appendix 2), using Eq. (2.19), and the orthogonality relations of the Chebyshev polynomials, one obtains [10]

$$(3.4) \quad T = \frac{-48}{p^4} \frac{\alpha_0}{2\pi}.$$

Substituting Eq. (3.4) in Eq. (3.1), one obtains the well-known Jost-Luttinger fourth-order result [11]

$$(3.5) \quad (Z_3^{-1})_{\text{div}}^{(4)} = \left(\frac{\alpha_0}{2\pi}\right)^2 \left[\ln \frac{M^2}{m^2} \right].$$

4. NUMBERS, LINKS, AND KNOTS

Kreimer has conjectured that the coefficient of the r th-order divergence for ladder graphs without crossed photon lines, namely the coefficient of $\left(\frac{\alpha_0}{2\pi}\right)^{r/2} \left[\ln \frac{M^2}{m^2} \right]$, should be a rational number [1]. This is in fact the case in Eq. (3.5) with the rational coefficient $C(Z_3^{-1})_{\text{div}}^{(4)}$ given by

$$(4.1) \quad C(Z_3^{-1})_{\text{div}}^{(4)} = 1.$$

The topology of the associated graph, Eq. (3.2), in Kreimer's framework, can be graphically represented as follows:

$$(4.2) \quad \text{Top}(Z_3^{-1})_{1\text{div}}^{(4)} \equiv \text{[Diagram of two linked loops]}$$

in which the clockwise oriented fermion momentum entering a vertex crosses over that exiting the vertex (for convenience, the convention here is opposite to that of Kreimer [1]). The resultant topology is that of a two-loop ladder, or Hopf link [12]. Every loop corresponds to a link. In general, a link is a possibly intertwined union of possible knotted loops in three dimensions. Here the two loops are both unknots. In Kreimer's scheme, any link resulting from a diagram with n loops must be skeined $n - 1$ times to complete the map to a knot [1]. This is motivated by the skein relation

(4.3)

$$\text{crossing} = \mathbf{A} \text{ (swapped crossing)} + \mathbf{B} \text{ (parallel lines)}$$

relating an oriented over crossing to a 'switch' and a 'splice' [13]. Each internal propagator in the Feynman diagram ends on two vertices, and one of the two is chosen to skein for each propagator. (In more general cases, no skeining is performed on mutual propagator crossings since the propagators can be drawn differently.) Thus, implementing the **B**-skein once for this case of two loops, Eq. (4.2) becomes

(4.4)

$$\text{Hopf link} \xrightarrow{\mathbf{B}} \text{figure-eight} \rightarrow \text{circle}$$

resulting in the unknot. (The **A**-skein, ignored here, produces terms mapping onto the antipode of the associated combinatorial Hopf algebra which picks up terms generated by the coproduct and combines them in the same way as the forest formula of renormalization theory [1].) Comparing Eqs. (3.2), (4.1), (4.2), and (4.4), one has the correspondences between the topology $\text{Top}(Z_3^{-1})_{1 \text{ div}}^{(4)}$ with no photon crossings, the rational number $C(Z_3^{-1})_{\text{div}}^{(4)} = 1 \in \mathbf{Q}$ (the set of rational numbers), and the trivial unknot, in accord with Kreimer's conjecture. It should be stressed that this procedure is rather ad hoc and is not derived from first principles. It has also been shown to fail at large loop orders [1]

5. PHYSICAL HEURISTICS

In the present work I argue that the mapping of the divergent part of Feynman diagrams onto links can be motivated by the following physical heuristics. At high energy, $k \rightarrow \infty$ (corresponding to extremely small distances), the photon propagator (ignoring the metric) can be rewritten as

$$(5.1) \quad \frac{1}{k^2} = -\lim_{m \rightarrow 0} \frac{1}{i\gamma k + m} \frac{1}{i\gamma k + m} = \frac{1}{i\gamma(-k)} \frac{1}{i\gamma k},$$

which is like two massless Fermion propagators with opposite Euclidean four-momenta. Diagrammatically, Eq. (5.1) can be represented by

$$\text{wavy line} \sim \text{two parallel lines with arrows}$$

(5.2)

in which at very small distances, the photon line is represented by two counter-propagating Fermion lines, namely an electron and a positron. Here one invokes Feynman's picture of a positron as an electron going backward in time [14]. Next, the electron photon interaction at a vertex for extremely small distances, can then be represented graphically by

$$(5.3) \quad \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \\ | \\ \text{~~~~~} \end{array} \sim \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \\ | \quad | \\ \text{---} \text{---} \end{array}$$

As in Eq. (4.2) invoking the crossing rule to connect the external and internal Fermion lines, one obtains

$$(5.4) \quad \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \\ \diagdown \quad \diagup \\ | \quad | \\ \text{---} \text{---} \end{array}$$

Thus an electron entering the vertex from the left crosses over an electron coming from the future (a positron), and the electron arriving at the interaction vertex backward in time from the future continues forward in time into the future. Applying the heuristic Eq. (5.4) to $\text{Top}(Z_3^{-1})_{1\text{div}}^{(4)}$, one obtains the mapping from the Feynman diagram onto a link (Note: the second diagram merely serves as a convenient guide for constructing the final diagram.):

$$(5.5) \quad \text{Top}(Z_3^{-1})_{1\text{div}}^{(4)} \equiv \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \\ | \\ \text{~~~~~} \end{array} \sim \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \\ | \quad | \\ \text{---} \text{---} \end{array} \sim \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \\ | \quad | \\ \text{---} \text{---} \end{array}$$

This is again the Hopf link. Here this is obtained by physical heuristics, whereas Kreimer obtains the Hopf link by identifying the two loops in the Feynman diagram and invoking his crossing rule. The physical heuristics given here motivates the mapping onto links, but the links must also still be skeined to yield a knot (in this case the unknot). (It should be noted that here and in [1], the locations of vertex gamma matrices are ignored in the topological mappings.) One may speculate that the skeining might also be motivated by physical heuristics based on the well-known direct and exchange amplitudes for electron scattering, namely,

$$(5.6) \quad \begin{array}{c} \uparrow \quad \uparrow \\ + \\ \text{X} \end{array}$$

6. SIXTH-ORDER DIVERGENCE

Proceeding with the sixth order calculation of $(Z_3^{-1})_{\text{div}}$, it can be shown from Eq. (2.18) that [10]

$$(6.1) \quad (Z_3^{-1})_{\text{div}}^{(6)} = -\frac{p^4}{48} \frac{\alpha_0}{2\pi} \ln \frac{M^2}{m^2} \sum_{i=1}^{14} T_i = \sum_{i=1}^{14} (Z_3^{-1})_{i \text{ div}}^{(6)}.$$

The fourteen terms $\{T_i, i = 1, 14\}$ in Eq. (6.1) are ordered as they were calculated in [10], but in the following these terms are addressed in a different order, namely, first the ladder graph T_1 ; next the two sets of graphs containing crossed photon lines (excluding self-energy insertions) $\{T_6, T_2, T_4\}$ and $\{T_3, T_5, T_7\}$; and then the remaining graphs $\{T_i, i = 8 - 14\}$.

The first term T_1 of the fourteen terms $\{T_i, i = 1 - 14\}$ in Eq. (6.1) can be represented graphically by

$$(6.2) \quad \frac{1}{2} T_1 = \text{[Diagram: A sum of four two-photon ladder topologies. Each diagram consists of two fermion lines (curly) connected by two photon lines (wavy). The first diagram has a vertical photon line, the second has a horizontal photon line, the third has a diagonal photon line, and the fourth has a vertical photon line with a different internal structure.]}$$

This has a two-photon ladder topology. Using the Feynman rules, it can be shown that [10]

$$(6.3) \quad T_1 = -\frac{1}{48p^4} \left[ie_0^2 \int \frac{d^4 p'}{(2\pi)^4} \frac{\text{Tr} (\gamma_\mu \gamma p \gamma_\alpha - \gamma_\alpha \gamma p \gamma_\mu) \gamma_\kappa (\gamma_\alpha \gamma p' \gamma_\mu - \gamma_\mu \gamma p' \gamma_\alpha) \gamma_\kappa}{2p'^4 (p - p')^2} \right]^2,$$

and using arguments involving Lorentz and charge-conjugation invariance, and again performing the trace, doing the Wick rotations, and using the Chebyshev expansion, one obtains [10]

$$(6.4) \quad T_1 = -\frac{48}{p^4} \left(\frac{\alpha_0}{2\pi} \right)^2.$$

Substituting Eq. (6.4) in Eq. (6.1), one obtains

$$(6.5) \quad (Z_3^{-1})_{1 \text{ div}}^{(6)} = \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

The coefficient of $\left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right]$ in Eq. (6.5) is rational, namely,

$$(6.6) \quad C (Z_3^{-1})_{1 \text{ div}}^{(6)} = 1.$$

Again using either Kreimer's mapping or that of the present author, the topology of the associated graph, Eq. (6.2) can be graphically represented as follows:

$$(6.7) \quad \text{Top } (Z_3^{-1})_{1 \text{ div}}^{(6)} \equiv \text{[Diagram: A sum of three topological representations of the two-photon ladder topology. The first is a standard ladder, the second is a crossed ladder, and the third is a more complex topology with multiple internal lines.]}$$

or

$$\text{Top } (Z_3^{-1})_{\text{div}}^{(6)} \equiv \text{Diagram of three overlapping circles} \quad (6.8)$$

In the Kreimer method, it is noted that the ladder topology of this Feynman graph has three loops, and the crossing rule is used to directly obtain the three-component Hopf link. Alternatively using the mapping unto links based on the physical heuristics of Eq. (5.4), one obtains the same three-component Hopf link. Next, the three component Hopf link can be skeined to obtain the unknot, consistent with the rational number Eq. (6.6).

7. APÉRY'S NUMBER AND THE TREFOIL KNOT

Next consider the term T_6 which contains crossed photon lines and has the Feynman diagrammatic representation:

$$T_6 = \text{Diagram 1} + \text{Diagram 2} + \text{Diagram 3} + \text{Diagram 4} \quad (7.1)$$

Using the Feynman rules, It can be shown that [10]:

$$\begin{aligned} T_6 = & 2\text{Tr}\gamma_\mu \frac{1}{i\gamma p} \int \frac{d^4 p'}{(2\pi)^4} \int \frac{d^4 q}{(2\pi)^4} (ie_0^2)^2 \gamma_\lambda \left[\frac{1}{i\gamma(p-q)} \gamma_\kappa \frac{1}{i\gamma(p'-q)} \right. \\ & \gamma_\mu \frac{1}{i\gamma(p'-q)} \gamma_\lambda \left(-\frac{\gamma p'}{p'^4} \right) \gamma_\kappa \frac{1}{i\gamma p} \frac{1}{q^2 (p-p')^2} \\ & - \left(\frac{1}{i\gamma(p-q)} \frac{\gamma_\alpha}{2} \frac{1}{\gamma(p-q)} \right) \gamma_\kappa \frac{1}{i\gamma(p'-q)} \gamma_\mu \frac{1}{i\gamma(p'-q)} \gamma_\lambda \\ & \left. \left(\frac{1}{i\gamma p'} \frac{\gamma_\alpha}{2} \frac{1}{\gamma p'} \right) \right]. \end{aligned} \quad (7.2)$$

Next rotating contours of integration, using the trace formulas and the algebra of the Dirac gamma matrices, performing Chebyshev expansions, using the orthogonality relations for the Chebyshev polynomials, and using the fact that the integral must be independent of the direction of the momentum p so that one can use the integral over a solid angle,

$$1 = \int \frac{d\Omega_p}{2\pi^2}, \quad (7.3)$$

it can be shown that [10]

$$T_6 = \frac{-96\zeta(3) + 72}{p^4} \left(\frac{\alpha_0}{2\pi} \right)^2. \quad (7.4)$$

Then substituting Eq. (7.4) in Eq. (6.1), one obtains

$$(Z_3^{-1})_{6\text{div}}^{(6)} = \left(-\frac{3}{2} + 2\zeta(3) \right) \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right]. \quad (7.5)$$

In this case the coefficient of $\left(\frac{\alpha_0}{2\pi}\right)^3 \left[\ln \frac{M^2}{m^2}\right]$ is

$$(7.6) \quad C(Z_3^{-1})_{6\text{div}}^{(6)} = -\frac{3}{2} - 2\zeta(3).$$

Thus this non-ladder crossed-photon topology yields an irrational coefficient containing Apéry's number [3], [4], the Riemann zeta function of three, $\zeta(3)$.

Recall that the Riemann zeta function $\zeta(s)$ is defined by the infinite series

$$(7.7) \quad \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

In particular, Apéry's number [15]

$$(7.8) \quad \zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$$

$$(7.9) \quad = 1.202056903159594285399738161511449990764986292....$$

was recently calculated to 10 billion digits [16]. In 1979 Roger Apéry proved that $\zeta(3)$ is an irrational number [3], namely,

$$(7.10) \quad \zeta(3) \notin \mathbb{Q},$$

and it is believed to be transcendental [1], although this has not been proven [4]. While the set of all rational numbers is countable, the set of reals is not countable. The set of irrational numbers, including the set of algebraic and transcendental numbers, is an uncountable set. In 1874, G. Cantor proved that most real numbers are transcendental [17]. However, proving that a number is transcendental is generally extremely difficult [18], [19], [20], [21]. Leonard Euler proved that the Riemann zeta functions $\zeta(n)$ for even $n \geq 2$ are proportional to π^n [22], [23], [24], namely,

$$(7.11) \quad \zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \dots$$

Furthermore Ferdinand Lindemann proved in 1882 that π is transcendental [25], from which it can be proved that $\zeta(n)$ for even $n \geq 2$ are transcendental [26]. However it has not been proven that $\zeta(n)$ for odd $n \geq 3$ are transcendental. Irrational numbers are either algebraic or transcendental, and to prove that an irrational number is transcendental one must prove that it is not the root of a polynomial equation with integer or rational coefficients. T. Ravaol proved that there are infinitely many integers n such that $\zeta(2n+1)$ is irrational [27], [24]. V. Zudilin proved that at least one of $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ is irrational [28]. Kreimer's correspondence between Feynman graphs which map onto knots and irrational (likely transcendental) numbers has been shown to include multiple sums (Euler-Zagier sums, multiple zeta values or multiple harmonic series) and is rich in number theory [1], [29], [24].

Using Kreimer's mapping method to reduce Eq. (7.1), one first notes that the three-loop topology of the graph is made transparent by the following identification:

$$\text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{Diagram 1} = \text{Diagram 2} = \text{Diagram 3}$$

which maps first into the following three loops:

$$(7.13) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{Diagram 4}$$

Then using the crossing rule, including the propagators which cross each other, produces three entangled Hopf links:

$$(7.14) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{Diagram 5}$$

Next, the **B**-skein performed twice yields

$$(7.15) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{Diagram 6} \rightarrow \text{Diagram 7}$$

which is clearly a trefoil knot, namely the right-handed type-(2,3) torus knot [12]. Thus the topology of the Feynman graph is that of the trefoil knot:

$$(7.16) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{Diagram 8}$$

Kreimer and Broadhurst [1] have shown that other higher-order Feynman graph topologies map onto other torus knots. They have shown that $\zeta(n)$ arises from the integrations, and the type-(2,n) torus knots result from the mappings.

If one uses instead the heuristic method introduced in the present work, one has

$$(7.17) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{Diagram 9} \sim \text{Diagram 10}$$

(The diagram on the right serves as a guide for constructing the next diagram.) Using Eq. (5.4) at each vertex, this becomes

$$(7.18) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{[Diagram: A complex knot with two loops and a central crossing, representing a trefoil knot.]}$$

The two electron-positron pairs replacing the two crossed photon lines are separated above and below each other, respectively. Slipping the upper central loop under the left loop, one obtains

$$(7.19) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{[Diagram: A trefoil knot, which is a single loop with three crossings.]}$$

which is again the trefoil knot

$$(7.20) \quad \text{Top } (Z_3^{-1})_{6\text{div}}^{(6)} \equiv \text{[Diagram: A trefoil knot, identical to the one in (7.19).]}$$

In this case, no skeining is needed.

8. MORE CROSSED PHOTON PROPAGATORS

Next, the term T_2 can be represented graphically by

(8.1)

$$\frac{1}{2} T_2 = \text{[Diagram: A sum of four Feynman diagrams. Each diagram shows a loop with two internal lines crossing each other, representing a crossed photon propagator.]}$$

which also has the same two crossed photon topology. It can be shown that [10]

$$(8.2) \quad \begin{aligned} T_2 &= 2\text{Tr} \frac{1}{i^2} \frac{(\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha)}{2p^4} \int \frac{d^4 q}{(2\pi)^4} \int \frac{d^4 p'}{(2\pi)^4} (ie_0^2)^2 \gamma_\kappa \\ &\quad \frac{1}{i\gamma(p-q)} \gamma_\rho \frac{1}{i^2} [\gamma_\mu \gamma(p'-q) \gamma_\alpha - \gamma_\alpha \gamma(p'-q) \gamma_\mu] \\ &\quad \frac{1}{2(p'-q)^4} \gamma_\kappa \frac{1}{i\gamma p'} \gamma_\rho \frac{1}{(p-p')^2 q^2}, \end{aligned}$$

which reduces to [10]

$$(8.3) \quad T_2 = -\frac{96}{p^4} \left(\frac{\alpha_0}{2\pi} \right)^2.$$

It is interesting to note that in performing the integral, Riemann zeta functions $\zeta(2)$ appear for different regions of integration but cancel when combined. Next substituting Eq. (8.3) in Eq. (6.1), one obtains

$$(8.4) \quad (Z_3^{-1})_{2\text{div}}^{(6)} = 2 \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

The coefficient of $\left(\frac{\alpha_0}{2\pi}\right)^3 \left[\ln \frac{M^2}{m^2}\right]$ in Eq. (8.4) is in this case rational, namely,

$$(8.5) \quad C(Z_3^{-1})_{2\text{div}}^{(6)} = 2.$$

Next since the topology of the graph Eq. (8.1) is the same as that of T_6 , Eq. (7.17), one again obtains the trefoil knot:

$$(8.6) \quad \text{Top}(Z_3^{-1})_{2\text{div}}^{(6)} \equiv \text{[Diagram 1]} \sim \text{[Diagram 2]}$$

or

$$(8.7) \quad \text{Top}(Z_3^{-1})_{2\text{div}}^{(6)} \equiv \text{[Diagram 3]} \rightarrow \text{[Diagram 4]}$$

or

$$(8.8) \quad \text{Top}(Z_3^{-1})_{2\text{div}}^{(6)} \equiv \text{[Trefoil Knot]}$$

Although the coefficient $C(Z_3^{-1})_{2\text{div}}^{(6)}$, Eq. (8.5), is rational while the topology is again that of the trefoil knot, it is to be realized that the sum of all of the coefficients corresponding to the topology in Eq. (8.6) will still be irrational (likely transcendental).

Next, the term T_4 can be represented graphically by

$$(8.9) \quad \frac{1}{4} T_4 = \text{[Diagram 5]} + \text{[Diagram 6]} + \text{[Diagram 7]} + \text{[Diagram 8]}$$

which also has the same two crossed photon topology. It can be shown that [10]

$$(8.10) \quad T_4 = 4 (ie_0^2)^2 \int \frac{d^4 q}{(2\pi)^4} \int \frac{d^4 p'}{(2\pi)^4} \text{Tr} \frac{1}{i^2} \frac{(\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha)}{2p^4} \left[\gamma_\lambda \frac{1}{i} \left(\frac{\gamma_\alpha}{2(p-q)^2} - \frac{(p_\alpha - q_\alpha) \gamma(p-q)}{(p-q)^4} \right) \gamma_\kappa \frac{1}{i \gamma(p'-q)} \gamma_\mu \right. \\ \left. \frac{1}{i \gamma(p'-q)} \gamma_\lambda \frac{1}{i \gamma p'} \frac{\gamma_\kappa}{(p-p')^2 q^2} + \gamma_\lambda \frac{1}{i \gamma(p-q)} \gamma_\kappa \frac{1}{i \gamma(p'-q)} \right. \\ \left. \gamma_\mu \frac{1}{i \gamma(p'-q)} \left(-\frac{\gamma_\alpha}{2p'^2} + \frac{p'_\alpha \gamma p'}{p'^4} \right) \frac{\gamma_\kappa}{(p-p')^2 q^2} \right],$$

for which all terms sum to zero [10],

$$(8.11) \quad T_4 = 0.$$

Substituting Eq. (8.11) in Eq. (6.1), one obtains

$$(8.12) \quad (Z_3^{-1})_{4 \text{ div}}^{(6)} = 0 \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

The coefficient of $\left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right]$ in Eq. (8.12) is in this case rational, namely,

$$(8.13) \quad C(Z_3^{-1})_{4 \text{ div}}^{(6)} = 0$$

Next since the topology of the graph Eq. (8.9) is again the same as that of T_6 , Eq. (7.17), one again obtains the trefoil knot:

$$(8.14) \quad \text{Top}(Z_3^{-1})_{4 \text{ div}}^{(6)} \equiv \text{Diagram} \rightarrow \text{Trefoil Knot}$$

Although the coefficient $C(Z_3^{-1})_{4 \text{ div}}^{(6)}$ is again rational while the topology is that of the trefoil knot, it is again to be realized that the sum of all of the coefficients corresponding to the same topology will still be irrational (likely transcendental).

Thus combining Eqs. (7.20), (8.8), and (8.14), one obtains

$$(8.15) \quad \text{Top}[(Z_3^{-1})_{2 \text{ div}}^{(6)} + (Z_3^{-1})_{4 \text{ div}}^{(6)} + (Z_3^{-1})_{6 \text{ div}}^{(6)}] \equiv \text{Diagram} \sim \text{Trefoil Knot}$$

Next combining Eqs. (8.5), (8.13), and (7.6), one has

$$(8.16) \quad C(\text{Trefoil Knot}) = C(Z_3^{-1})_{2 \text{ div}}^{(6)} + C(Z_3^{-1})_{4 \text{ div}}^{(6)} + C(Z_3^{-1})_{6 \text{ div}}^{(6)}$$

or

$$(8.17) \quad C(\text{Trefoil Knot}) = 2 + 0 + \left(-\frac{3}{2} + 2\zeta(3)\right) = \frac{1}{2} + 2\zeta(3)$$

Thus the overall coefficient Eq. (8.17) for the trefoil knot topology, arising from Eqs. (7.1), (8.1), and (8.9), includes Apéry's number $\zeta(3)$ which is irrational and likely transcendental, consistent with Kreimer's conjecture associating Feynman diagrams, transcendental numbers, and knots.

Next consider the term T_3 , which also contains crossed photon lines but has a different Feynman diagrammatic representation from that of Eqs. (7.1), (8.1), and (8.9):

$$(8.18) \quad \frac{1}{4} T_3 = \text{[Diagram 1]} + \text{[Diagram 2]} + \text{[Diagram 3]} + \text{[Diagram 4]}$$

The ‘blob’ vertex represents the third-order vertex with another third-order vertex subtracted out, but with the same Fermion momentum entering and leaving its internal first-order vertex, and is graphically represented by

$$(8.19) \quad \text{[Diagram 1]} \equiv \text{[Diagram 2]} - \text{[Diagram 3]} \equiv \text{[Diagram 4]} - \text{[Diagram 5]}$$

To compensate for the subtraction (introduced for computational convenience), the same term is added as T_8 [See Eq. (9.1)]. It can be shown that [10]:

$$(8.20) \quad T_3 = 4\text{Tr} \frac{1}{i^2} \frac{(\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha)}{2p^4} \int \frac{d^4 q}{(2\pi)^4} \int \frac{d^4 p'}{(2\pi)^4} (ie_0^2)^2 \left[\gamma_\kappa \frac{1}{i\gamma(p-q)} \gamma_\rho \frac{1}{i\gamma(p'-q)} \gamma_\kappa - \gamma_\kappa \frac{1}{i\gamma(p-q)} \gamma_\rho \frac{1}{i\gamma(p-q)} \gamma_\kappa \right] \frac{1}{i^2} \frac{(\gamma_\mu \gamma p' \gamma_\alpha - \gamma_\alpha \gamma p' \gamma_\mu) \gamma_\rho}{2p^4 q^2 (p-p')^2}.$$

Next rotating contours of integration, using the trace formulas and the algebra of the Dirac gamma matrices, performing Chebyshev expansions, using the orthogonality relations for the Chebyshev polynomials, and using the fact that the integral must be independent of the direction of the momentum p so that one can use the integral over a solid angle,

$$(8.21) \quad 1 = \int \frac{d\Omega_p}{2\pi^2},$$

it can be shown that [10]

$$(8.22) \quad T_3 = \frac{96\zeta(3) + 16}{p^4} \left(\frac{\alpha_0}{2\pi} \right)^2.$$

Logarithmic divergences, $\ln(M/p)$, appear at intermediate stages in the integration but all cancel. Next substituting Eq. (8.22) in Eq. (6.1), one obtains

$$(8.23) \quad (Z_3^{-1})_{3\text{div}}^{(6)} = \left(-\frac{1}{3} - 2\zeta(3) \right) \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

In this case the coefficient of $\left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right]$ is

$$(8.24) \quad C (Z_3^{-1})_{3\text{div}}^{(6)} = -\frac{1}{3} - 2\zeta(3).$$

Thus this non-ladder crossed-photon topology also yields an irrational coefficient containing Apéry's number $\zeta(3)$. Next one first notes that the topology of the graph is equivalent to that of Eq. (7.17). Thus

$$\text{Top } (Z_3^{-1})_{3\text{div}}^{(6)} \equiv \text{Diagram 1} \sim \text{Diagram 2} \quad (8.25)$$

The equivalence is justified by Kreimer's topological mapping procedure, in which vertices are ignored. (However the location of the vertices is displayed here for further consideration at the end of this section.) It then follows from Eqs. (8.25) and (8.14) that

$$\text{Top } (Z_3^{-1})_{3\text{div}}^{(6)} \equiv \text{Diagram 3} \quad (8.26)$$

Thus one again obtains the right-handed trefoil knot.

Next, the term T_5 can be represented graphically by

$$\frac{1}{8} T_5 = \text{Diagram 4a} + \text{Diagram 4b} + \text{Diagram 4c} + \text{Diagram 4d} \quad (8.27)$$

which also has the same two crossed photon topology as Eq. (8.18). It can be

shown that [10]

$$\begin{aligned} T_5 \sim & \gamma_\kappa \gamma_\alpha \gamma_\lambda \gamma (p' - q) \gamma_\kappa \gamma_{p'} \gamma_\mu \gamma_{p'} \gamma_\lambda - \gamma_\kappa \gamma_\mu \gamma_\lambda \gamma (p' - q) \\ & \gamma_\kappa \gamma_{p'} \gamma_\alpha \gamma_{p'} \gamma_\lambda + \gamma_\kappa \gamma (p - q) \gamma_\lambda \gamma_\alpha \gamma_\kappa \gamma_{p'} \gamma_\mu \gamma_{p'} \gamma_\lambda \\ & - \gamma_\kappa \gamma (p - q) \gamma_\lambda \gamma_\mu \gamma_\kappa \gamma_{p'} \gamma_\alpha \gamma_{p'} \gamma_\lambda, \end{aligned} \quad (8.28)$$

and using the algebra of the Dirac gamma matrices (Appendix 1), Eq. (8.28) is seen to be vanishing, thus

$$T_5 = 0. \quad (8.29)$$

It then follows that

$$(Z_3^{-1})_{5\text{div}}^{(6)} = 0 \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right], \quad (8.30)$$

and

$$(8.31) \quad C \left(Z_3^{-1} \right)_{5 \text{ div}}^{(6)} = 0.$$

Next since the topology of the graph Eq. (8.27) is the same as that of T_3 , Eq. (8.18), one again obtains the trefoil knot:

$$(8.32) \quad \text{Top} \left(Z_3^{-1} \right)_{5 \text{ div}}^{(6)} \equiv \text{[Diagram: A graph with two vertices and three internal lines, one of which is a loop, connected to form a trefoil knot]} \rightarrow \text{[Diagram: A trefoil knot]}.$$

Although the coefficient $C \left(Z_3^{-1} \right)_{5 \text{ div}}^{(6)}$ is rational while the topology is again that of the trefoil knot, it is again to be realized that the sum of all of the coefficients corresponding to the same topology as Eq. (8.27) will still be irrational (likely transcendental).

Next, the term T_7 can be represented graphically by

$$(8.33) \quad \frac{1}{2} T_7 = \text{[Diagram: Four identical graphs, each with two vertices and three internal lines, one of which is a loop, connected to form a trefoil knot]}.$$

which again has the same two crossed-photon topology. It can be shown that [10]

$$(8.34) \quad \begin{aligned} T_7 = & 2 \text{Tr} \gamma_\mu \frac{1}{i\gamma p} \int \frac{d^4 p'}{(2\pi)^4} \int \frac{d^4 q}{(2\pi)^4} (ie_0^2)^2 \gamma_\kappa \\ & \left[\left(\frac{-\gamma(p-q)}{i(p-q)^4} \right) \gamma_\lambda \frac{1}{i\gamma(p'-q)} + 2 \left(\frac{-1}{i\gamma(p-q)} \frac{\gamma_\alpha}{2} \frac{1}{\gamma(p-q)} \right) \right. \\ & \gamma_\lambda \left(\frac{-1}{i\gamma(p'-q)} \frac{\gamma_\alpha}{2} \frac{1}{\gamma(p'-q)} \right) + \left. \frac{1}{i\gamma(p-q)} \gamma_\lambda \left(\frac{-\gamma(p'-q)}{i(p'-q)^4} \right) \right] \\ & \gamma_\kappa \frac{1}{i\gamma p'} \gamma_\mu \frac{1}{i\gamma p'} \gamma_\lambda \frac{1}{i\gamma p} \frac{1}{q^2 (p-p')^2}. \end{aligned}$$

Evaluating the integral, it can be shown that [10],

$$(8.35) \quad T_7 = \frac{8}{p^4} \left(\frac{\alpha_0}{2\pi} \right)^2.$$

Although Apéry's number $\zeta(3)$ appears at intermediate stages of the calculation of Eq. (8.34), it is canceled out. Substituting Eq. (8.35) in Eq. (6.1), one obtains

$$(8.36) \quad \left(Z_3^{-1} \right)_{7 \text{ div}}^{(6)} = -\frac{1}{6} \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

The coefficient of $\left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right]$ in Eq. (8.36) is in this case rational, namely,

$$(8.37) \quad C \left(Z_3^{-1} \right)_{7 \text{ div}}^{(6)} = -\frac{1}{6}.$$




Next since the topology of the graph Eq. (8.33) is again the same as that of T_3 , Eq. (80), one again obtains the trefoil knot:

(8.38)

$$\text{Top} (Z_3^{-1})_{7\text{div}}^{(6)} \equiv \text{Diagram 1} \sim \text{Diagram 2} \rightarrow \text{Diagram 3}$$




Thus combining Eqs. (8.26), (8.32), and (8.38), one obtains
(8.39)

$$\text{Top} \left[(Z_3^{-1})_{3\text{div}}^{(6)} + (Z_3^{-1})_{5\text{div}}^{(6)} + (Z_3^{-1})_{7\text{div}}^{(6)} \right] \equiv \text{Diagram 1} \sim \text{Diagram 2} \rightarrow \text{Diagram 3}$$




Combining Eqs. (8.24), (8.31), and (8.37), one has

$$C(\text{Trefoil}) = C(Z_3^{-1})_{3\text{div}}^{(6)} + C(Z_3^{-1})_{5\text{div}}^{(6)} + C(Z_3^{-1})_{7\text{div}}^{(6)} \quad (8.40)$$

or

$$C(\text{Trefoil}) = \left(-\frac{1}{3} - 2\zeta(3)\right) + 0 + \left(-\frac{1}{6}\right) = -\frac{1}{2} - 2\zeta(3) \quad (8.41)$$

Thus the overall coefficient Eq. (8.41) for the trefoil knot topology, arising from Eqs. (8.18), (8.27), and (8.33), again includes Apéry's number $\zeta(3)$ which is irrational and likely transcendental.

But combining Eqs. (8.17) and (8.41), explicitly displaying the unreduced topologies, one has an overall cancellation of Apéry's number, namely,

$$C(\text{Diagram 1}) + C(\text{Diagram 2}) = 0 \quad (8.42)$$



The overall cancellation of $\zeta(3)$ was evident in early work [7], [10]. Much later Broadhurst and Kreimer argued that this cancellation of transcendentals also follows from gauge symmetry (Ward identity) together with skein relations [1]. This fact challenges Kreimer's conjectured correspondence between graphs yielding knots and transcendental numbers. However it is appropriate to recall that in identifying the topologies of the two crossed-photon graphs in Eq. (8.25), the vertices were ignored. This suggests that by generalizing the graph 'topology' to distinguish the location of the gamma matrices at the vertices, the correspondence with transcendentals could possibly be maintained.

9. REMAINING SIXTH-ORDER TERMS

The remaining graphs $T_8 - T_{14}$ are of little importance to the present work because they produce no transcendentals. However for completeness they are briefly addressed in the following. First, the term T_8 can be represented graphically by

$$\frac{1}{4} T_8 = \text{[Four diagrams: each is a circle with a vertical wavy line and a small loop on top, with various external lines]} \quad (9.1)$$

This term was included to cancel the subtracted term introduced previously in Eqs. (8.18) and (8.19). It can be shown that [10]

$$T_8 = 4\text{Tr} \int \frac{d^4 q}{(2\pi)^4} \frac{1}{i^2 2p^4 q^2 i^2 2(p-q)^4} i e_0^2 (\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha) \\ \left(B^{(2)}(p^2) \gamma_\beta + 2p_\beta \gamma p B^{(2)'}(p^2) \right) \\ (\gamma_\mu \gamma(p-q) \gamma_\alpha - \gamma_\alpha(p-q) \gamma_\mu) \gamma_\beta, \quad (9.2)$$

in which $B^{(2)}(p^2)$ is defined below in Eq. (9.8), and $B^{(2)'}(p^2)$ denotes its derivative. In obtaining Eq. (9.2), the Ward identity [5]

$$i(p-p')\Gamma^\mu(p',p) = S^{-1}(p') - S^{-1}(p) \quad (9.3)$$

was used for the third-order vertex $\Gamma_\mu^{(3)}(p,p)$, namely,

$$\Gamma_\mu^{(3)}(p,p) = \Gamma_\mu(p,p) - \gamma_\mu = \frac{1}{i} \frac{\partial}{\partial p^\mu} S^{-1}(p), \quad (9.4)$$

in which the inverse electron propagator $S^{-1}(p)$ with bare mass $m_0 = 0$ is

$$S^{-1}(p) = i\gamma p + \Sigma, \quad (9.5)$$

where Σ is the electron self energy. Equation (9.2) reduces to [10]

$$T_8 = -\frac{96}{p^4} \frac{\alpha_0}{2\pi} \left[B^{(2)}(p^2) + p^2 B^{(2)'}(p^2) \right]. \quad (9.6)$$

Here $B^{(2)}(p^2)$ is the second-order self-energy of the electron, graphically represented by

$$\frac{\gamma p}{i} B^{(2)}(p^2) = \text{[Diagram: a horizontal line with a wavy loop above it]} \quad (9.7)$$

and calculated to be [10]

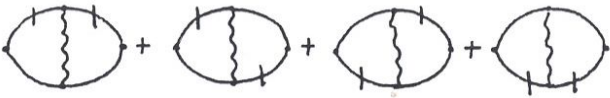
$$B^{(2)}(p^2) = \frac{3}{4} \left(\frac{\alpha_0}{2\pi} \right) \left(-\frac{2}{3} \ln \left(\frac{p}{M} \right)^2 + 1 \right). \quad (9.8)$$

Substituting Eq. (9.6) in Eq. (6.1), one obtains

$$(9.9) \quad (Z_3^{-1})_{8 \text{ div}}^{(6)} = 2 \left[B^{(2)}(p^2) + p^2 B^{(2)'}(p^2) \right] \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

The occurrence of the higher order logarithmic divergences arises from the use of the Feynman gauge instead of the generalized Landau gauge which was used in [7]. However as shown in the following there is an overall cancellation of these higher order divergences in [10] and in the present work. For this reason and because no transcendental numbers arise, $C(Z_3^{-1})_{i \text{ div}}^{(6)}$ and $\text{Top}(Z_3^{-1})_{i \text{ div}}^{(6)}$ for $i = 8, 9, \dots, 14$, are ignored in the following.

Next, the terms T_9 and T_{10} can be represented graphically by

$$(9.10) \quad -\frac{1}{2} [B(p^2)]^{-1} T_9 = \frac{1}{4} [B^{(2)'}(p^2) p^\mu p^\nu]^{-1} T_{10}$$


It can be shown that [10]

$$(9.11) \quad \begin{aligned} T_9 &= -2B^{(2)}(p^2) \text{Tr} \int \frac{d^4 q}{(2\pi)^4} \frac{1}{2p^4 i^2 q^2 2(p-q)^4 i^2} \\ &\quad i e_0^2 (\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha) \gamma_\beta \\ &\quad (\gamma_\mu \gamma(p-q) \gamma_\alpha - \gamma_\alpha \gamma(p-q) \gamma_\mu) \gamma_\beta, \end{aligned}$$

which when evaluated yields

$$(9.12) \quad T_9 = \frac{48}{p^4} \frac{\alpha_0}{2\pi} B^{(2)}(p^2),$$

and

$$(9.13) \quad (Z_3^{-1})_{9 \text{ div}}^{(6)} = -B^{(2)}(p^2) \left(\frac{\alpha_0}{2\pi} \right)^2 \left[\ln \frac{M^2}{m^2} \right].$$

Also, It can be shown that [10]

$$(9.14) \quad T_{10} \sim (\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha) p^\mu,$$

which when evaluated yields

$$(9.15) \quad T_{10} = 0,$$

and

$$(9.16) \quad (Z_3^{-1})_{10 \text{ div}}^{(6)} = 0 \left(\frac{\alpha_0}{2\pi} \right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

Next, the term T_{11} can be represented graphically by

$$T_{11} = \begin{array}{c} \text{diagram 1} + \text{diagram 2} + \text{diagram 3} + \text{diagram 4} \\ + \text{diagram 5} + \text{diagram 6} + \text{diagram 7} + \text{diagram 8} \\ + \text{diagram 9} + \text{diagram 10} + \text{diagram 11} + \text{diagram 12} \end{array}$$

(9.17)

It can be shown that [10]

$$(9.18) \quad T_{11} = -2\text{Tr} \int \frac{d^4 q}{(2\pi)^4} \frac{1}{2p^4 i^2 q^2 2(p-q)^4 i^2} i e_0^2 (\gamma_\alpha \gamma p \gamma_\mu - \gamma_\mu \gamma p \gamma_\alpha) \gamma_\beta B^{(2)}((p-q)^2) (\gamma_\mu \gamma(p-q) \gamma_\alpha - \gamma_\alpha \gamma(p-q) \gamma_\mu) \gamma_\beta,$$

which when evaluated yields

$$(9.19) \quad T_{11} = \frac{48}{p^4} \frac{\alpha_0}{2\pi} B^{(2)}(p^2),$$

and

$$(9.20) \quad (Z_3^{-1})_{11 \text{ div}}^{(6)} = -B^{(2)}(p^2) \left(\frac{\alpha_0}{2\pi} \right)^2 \left[\ln \frac{M^2}{m^2} \right].$$

Next, the term T_{12} can be represented graphically by

$$[\{4B^{(4)'}(p^2) + 4p^2(B^{(2)'}(p^2))^2 - 4B^{(2)}(p^2)B^{(2)'}(p^2)\}p^\mu p^\nu]^{-1} T_{12} =$$

$$\begin{array}{c} \text{diagram 1} + \text{diagram 2} + \text{diagram 3} + \text{diagram 4} \end{array}$$

(9.21)

It can be shown that [10]

$$(9.22) \quad T_{12} = \frac{16}{p^4} \left[B^{(4)'}(p^2) + p^2(B^{(2)'}(p^2))^2 - B^{(2)}(p^2)B^{(2)'}(p^2) \right].$$

Here $B^{(4)}(p^2)$ is the fourth-order self-energy of the electron, graphically represented by

(9.23)

$$\frac{\gamma p}{i} B^{(4)}(p^2) = \begin{array}{c} \text{diagram 1} + \text{diagram 2} + \text{diagram 3} \end{array}$$

and calculated to be [10]

$$(9.24) \quad B^{(4)}(p^2) = \frac{9}{16} \left(\frac{\alpha_0}{2\pi} \right)^2 \left[\frac{2}{9} \left(\ln \left(\frac{p}{M} \right)^2 \right)^2 + \frac{4}{3} \ln \left(\frac{p}{M} \right)^2 - \frac{4}{3} \right].$$

It follows that

$$(9.25) \quad (Z_3^{-1})_{12 \text{ div}}^{(6)} = -\frac{1}{3} \left[B^{(4)'}(p^2) + p^2 (B^{(2)'}(p^2))^2 - B^{(2)}(p^2) B^{(2)'}(p^2) \right] \left(\frac{\alpha_0}{2\pi} \right) \left[\ln \frac{M^2}{m^2} \right].$$

Next, the terms T_{13} and T_{14} can be represented graphically by

$$(9.26) \quad \begin{aligned} & [\{2B^{(2)}(p^2)B^{(2)''}(p^2) - 2B^{(4)''}(p^2) + 2(B^{(2)'}(p^2))^2\}p^2 \\ & \quad + 4B^{(2)}(p^2)B^{(2)'}(p^2) - 4B^{(4)'}(p^2)]^{-1} T_{13} \\ & = -\frac{1}{4} [\{2B^{(2)''}(p^2)p^2 + 4B^{(2)'}(p^2)\}B^{(2)'}(p^2)p^\mu p^\nu]^{-1} T_{14} \\ & = \text{Diagram: A loop with two external lines, representing a photon propagator with a fermion loop insertion.} \end{aligned}$$

T_{13} is calculated to be [10]

$$(9.27) \quad T_{13} = \frac{8}{p^2} \left[2B^{(2)}(p^2)B^{(2)''}(p^2)p^2 - 2B^{(4)''}(p^2)p^2 + 2(B^{(2)'}(p^2))^2p^2 + 4B^{(2)}(p^2)B^{(2)'}(p^2) - 4B^{(4)'}(p^2) \right],$$

and it follows that

$$(9.28) \quad (Z_3^{-1})_{13 \text{ div}}^{(6)} = -\frac{p^2}{6} \left[2B^{(2)}(p^2)B^{(2)''}(p^2)p^2 - 2B^{(4)''}(p^2)p^2 + 2(B^{(2)'}(p^2))^2p^2 + 4B^{(2)}(p^2)B^{(2)'}(p^2) - 4B^{(4)'}(p^2) \right] \left(\frac{\alpha_0}{2\pi} \right) \left[\ln \frac{M^2}{m^2} \right].$$

T_{14} is calculated to be [10]

$$(9.29) \quad T_{14} = 16[2B^{(2)''}(p^2)p^2 + 4B^{(2)'}(p^2)]B^{(2)'}(p^2),$$

and it follows that

$$(9.30) \quad (Z_3^{-1})_{14 \text{ div}}^{(6)} = -\frac{p^4}{3} [2B^{(2)''}(p^2)p^2 + 4B^{(2)'}(p^2)]B^{(2)'}(p^2) \left(\frac{\alpha_0}{2\pi} \right) \left[\ln \frac{M^2}{m^2} \right].$$

Issue may be taken with the appearance of crossed-photon propagators in the second term of Eq. (9.23), and entering in Eqs. (9.27) and (9.28), evidently arising from the sixth and tenth graphs in Eq. (2.15). However none of the divergences in Eqs. (9.9), (9.13), (9.16), (9.20), (9.25), (9.28), and (9.30) contain Apéry's number, and when they are summed, they yield a rational coefficient of $\left(\frac{\alpha_0}{2\pi}\right)^3 \left(\ln \frac{M^2}{m^2}\right)$ [see Eq. (10.2)].

10. TOTAL SIXTH-ORDER DIVERGENCE

Next combining Eqs. (6.5), (8.4), (8.23), (8.12), (8.30), (7.5) and (8.36), one obtains

$$(10.1) \quad \sum_{i=1}^7 (Z_3^{-1})_{i \text{ div}}^{(6)} = \left(\frac{\alpha_0}{2\pi}\right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

The over-all coefficient 1 is due only to T_1 , namely the ladder graph. Also, combining Eqs. (9.9), (9.13), (9.16), (9.20), (9.25), (19.28), and (9.30), one obtains

$$(10.2) \quad \sum_{i=8}^{14} (Z_3^{-1})_{i \text{ div}}^{(6)} = -\frac{5}{4} \left(\frac{\alpha_0}{2\pi}\right)^3 \left[\ln \frac{M^2}{m^2} \right].$$

Combining Eqs. (10.1) and (10.2), one finally obtains

$$(10.3) \quad \sum_{i=8}^{14} (Z_3^{-1})_{i \text{ div}}^{(6)} = -\frac{1}{4} \left(\frac{\alpha_0}{2\pi}\right)^3 \left[\ln \frac{M^2}{m^2} \right],$$

in agreement with Rosner [7] who worked in a generalized Landau gauge. Since the result is the same in the Feynman gauge, this is consistent with gauge invariance, even though gauge invariance is lost at intermediate steps [10].

11. CONCLUSION

In the above, a review is given of the divergent part of the inverse charge renormalization constant in quantum electrodynamics calculated in Feynman gauge in fourth and sixth order in the bare charge of the electron. Certain graphs with crossed photon propagators are shown to yield Apéry's number, and topological mappings of those graphs onto the trefoil knot are investigated. A new mapping of graphs onto links and knots is given, based on physical heuristics. This model map is formulated by treating the asymptotic photon propagator as composite electron and positron propagators, and exploiting Feynman's picture of positrons as electrons moving backward in time. Also, the gauge invariant vanishing of the overall coefficient of Apéry's number is addressed.

12. APPENDIX 1 DIRAC MATRIX ALGEBRA AND TRACES

Useful algebra involving the Dirac gamma matrices γ_μ is as follows [30]:

$$(12.1) \quad \{\gamma_\mu, \gamma_\nu\} = 2g_{\mu\nu},$$

$$(12.2) \quad \gamma_\mu \gamma^\mu = 4,$$

$$(12.3) \quad \gamma_\mu \gamma a \gamma^\mu = -2\gamma a,$$

$$(12.4) \quad \gamma_\mu \gamma a \gamma b \gamma^\mu = 4a \cdot b,$$

$$(12.5) \quad \gamma_\mu \gamma a \gamma b \gamma c \gamma^\mu = -2\gamma c \gamma b \gamma a,$$

$$(12.6) \quad \gamma_\mu \gamma a \gamma b \gamma c \gamma d \gamma^\mu = 2(\gamma d \gamma a \gamma b \gamma c + \gamma c \gamma b \gamma a \gamma d).$$

Useful trace relations are:

$$(12.7) \quad \text{Tr} \gamma a \gamma b = 4a \cdot b,$$

$$(12.8) \quad \text{Tr} \gamma a_1 \gamma a_2 \dots \gamma a_{2n+1} = 0,$$

$$(12.9) \quad \text{Tr} \gamma a_1 \gamma a_2 \gamma a_3 \gamma a_4 = 4(a_1 \cdot a_2 \ a_3 \cdot a_4 + a_1 \cdot a_4 \ a_2 \cdot a_3 - a_1 \cdot a_3 \ a_2 \cdot a_4).$$

13. APPENDIX 2 CHEBYSHEV POLYNOMIAL EXPANSION

The Chebyshev polynomial expansion for momentum-difference denominators is given by [31]

$$(13.1) \quad \frac{\cos^m pp'}{(p-p')^{2k}} = \sum_{n=0}^{\infty} \left(\begin{matrix} m & k \\ p & p' \end{matrix} \right)_n C_n(pp'),$$

where pp' denotes the angle between the Euclidean four-momentum vectors p and p' , $C_n(pp')$ are the Chebyshev polynomials,

$$(13.2) \quad C_n(pp') = \frac{\sin((n+1)pp')}{\sin(pp')},$$

and $\left(\begin{matrix} m & k \\ p & p' \end{matrix} \right)_n$ are the Chebyshev coefficients. The orthogonality relations for the Chebyshev coefficients are given by

$$(13.3) \quad \int \frac{d\Omega_q}{2\pi^2} C_n(pq) C_m(p'q) = \frac{\delta_{nm}}{n+1} C_n(pp').$$

References

- [1] D. Kreimer, *Knots and Feynman Diagrams*, Cambridge University Press (2000).
- [2] D. Kreimer, "Dyson-Schwinger Equations: From Hopf Algebras to Number Theory," in *Universality and Renormalization*, I. Binder, D. Kreimer, Editors, Fields Institute Communications, American Mathematical Society, 2007 (pp. 225-248).
- [3] R. Apéry, *Asterisque* **61**, 11 (1979).
- [4] J. H. Conway and R. K. Guy, *The Book of Numbers*, Copernicus, New York (1996).
- [5] J. D. Bjorken and S. D. Drell, *Relativistic Quantum Fields*, McGraw Hill, New York (1965).
- [6] S. S. Schweber, *An Introduction to Relativistic Quantum Field Theory*, Harper and Row, New York (1961).
- [7] J. Rosner, *Ann. Phys.* **44**, 11 (1967).
- [8] K. Johnson, R. Willey, M. Baker, *Phys. Rev.* **163**, 1699 (1967).
- [9] M. Baker, K. Johnson, *Phys. Rev.* **183**, 1292 (1969).
- [10] Howard E. Brandt, *Sixth Order Charge Renormalization Constant*, Doctoral Thesis, University of Washington, Seattle, Washington (1970).
- [11] R. Jost and J. M. Luttinger, *Helv. Phys. Acta* **23**, 201 (1950).
- [12] D. Rolfsen, *Knots and Links*, Publish or Perish, Inc., Berkeley, California (1976).
- [13] L. H. Kauffman, *Knots and Physics*, 3rd Edition, World Scientific, Singapore (2001).
- [14] R. P. Feynman, *Phys. Rev.* **76**, 749 (1949).
- [15] S. R. Finch, *Mathematical Constants*, Cambridge University Press (2003).
- [16] S. Kondo and S. Pagliarulo, Apéry's constant in Wikipedia, <http://www.wikipedia.org/>, and <http://ja0hxxv.calico.jp/pai/eze3val.html> (2006).
- [17] G. Cantor, *Crelles Journal für die reine und angew. Mathem.*, Bd. 77 (1874).
- [18] A. Baker, *Transcendental Number Theory*, Cambridge University Press (1990).
- [19] S. Lang, *Introduction to Transcendental Numbers*, Addison-Wesley, Reading, Massachusetts (1966).
- [20] K. Mahler, *Lectures on Transcendental Numbers*, Lecture Notes on Mathematics, Springer-Verlag, New York (1976).
- [21] A. O. Gelfond, *Transcendental and Algebraic Numbers*, Dover Publications, New York (1960).
- [22] L. Euler, *Opera Omnia* I-14 (1734/5), 73-86.
- [23] V. S. Varadarajan, *Bull. Am. Math. Soc.* **44**, 515-539 (2007).
- [24] V. S. Varadarajan, *Euler Through Time: A New Look at Old Themes*, American Mathematical Society (2006).

- [25] F. Lindemann, Math. Ann. **20**, 213-225 (1882).
- [26] G. A. Jones and J. M. Jones, Elementary Number Theory, Springer Verlag, London, 1998 (pp. 179, 278).
- [27] T. Rivoal, C. R. Acad. Sci. Paris. Ser. I Math. **331**:4, 267-270 (2000).
- [28] V. V. Zudilin, Uspekhi Mat. Nauk **56**:4, 149-150 (2001); English transl., Russian Math. Surveys **56**, 774-776 (2001).
- [29] M. Kontsevich and D. Zagier, "Periods" in Mathematics Unlimited - 2001 and Beyond, B. Engquist and W. Schmid, Editors, Springer, New York, 2001 (pp. 771-808).
- [30] E. Caianiello, Nuovo Cimento **9**, 12, 214 (1953).
- [31] Handbook of Mathematical Functions, M. Abramowitz and I. A. Stegun, Editors, National Bureau of Standards, Applied Mathematics Series 55, U. S. Government Printing Office, Washington DC (1972).

U.S. ARMY RESEARCH LABORATORY, ADELPHI, MD
E-mail address: `hbrandt@arl.army.mil`

This page intentionally left blank

Braid Group, Temperley-Lieb Algebra, and Quantum Information and Computation

Yong Zhang

ABSTRACT. In this paper, we explore algebraic structures and low dimensional topology underlying quantum information and computation. We revisit quantum teleportation from the perspective of the braid group, the symmetric group and the virtual braid group, and propose the braid teleportation, the teleportation swapping and the virtual braid teleportation, respectively. Besides, we present a physical interpretation for the braid teleportation and explain it as a sort of crossed measurement. On the other hand, we propose the extended Temperley–Lieb diagrammatical approach to various topics including quantum teleportation, entanglement swapping, universal quantum computation, quantum information flow, and etc. The extended Temperley–Lieb diagrammatical rules are devised to present a diagrammatical representation for the extended Temperley–Lieb category which is the collection of all the Temperley–Lieb algebras with local unitary transformations. In this approach, various descriptions of quantum teleportation are unified in a diagrammatical sense, universal quantum computation is performed with the help of topological-like features, and quantum information flow is recast in a correct formulation. In other words, we propose the extended Temperley–Lieb category as a mathematical framework to describe quantum information and computation involving maximally entangled states and local unitary transformations.

1. Introduction

Quantum entanglements [1] play key roles in quantum information and computation [2, 3] and are widely exploited in quantum algorithms [4, 5], quantum cryptography [6, 7] and quantum teleportation [8, 9]. On the other hand, topological entanglements [10] denote topological configurations like links or knots which are closures of braids. Aravind [11] observed that there are natural similarities between quantum entanglements and topological entanglements. As a unitary braid has the power of detecting knots or links, it can often transform a separate quantum state into an entangled one. Kauffman and Lomonaco [12, 13] identified a nontrivial unitary braid representation with a universal quantum gate [14]. Recently, a series of papers have been published on the application of the braid group [10] (or the Yang–Baxter equation [15, 16]) to quantum information and computation, see [13, 17, 18] for unitary solutions of the Yang–Baxter equation as universal quantum gates; see [19, 20, 21] for quantum topology and quantum computation; see

1991 *Mathematics Subject Classification.* 81P68(Primary) 20F36, 18B99(Secondary).

Key words and phrases. Teleportation, Braid group, Temperley–Lieb algebra.

[22, 23] for quantum entanglements and topological entanglements; see for quantum algebras associated with maximally entangled states [24, 25, 26]; see [27, 28] for quantum error correction, topological quantum computing and a possible link between them.

We focus on the project of setting up a bridge between low dimensional topology and quantum information, namely looking for low dimensional topology underlying quantum information and computation. Kauffman's observation on the teleportation topology [13, 29] motivates our tour of revisiting in a diagrammatical approach all tight teleportation and dense coding schemes in Werner's work [30]. In a joint article with Kauffman and Werner [31], we make a survey of diagrammatical tensor calculus and matrix representations, and explore topological and algebraic structures underlying multipartite entanglements. In this article as a further extension of our work [32, 33, 34], we describe quantum information and computation (especially quantum teleportation [8, 9]) in the language of the braid group and Temperley–Lieb (TL) algebra [35]. We propose *the braid teleportation*, *teleportation swapping* and *virtual braid teleportation*, and devise *the extended TL diagrammatical rules* to describe quantum teleportation, entanglement swapping, universal quantum computation and quantum information flow.

Quantum teleportation is a procedure of sending a message from Charlie to Bob with the help of Alice. She shares a maximally entangled state (for example, Bell states [36]) with Bob, and performs an entangling measurement on the composite system between Charlie and Alice. After Bob gets results of Alice's measurement, he is able to obtain the message by exploiting the protocol between Alice and him. The transformation matrix between Bell states and product basis is found out to form a unitary braid representation [13], and it inspires us to reformulate *the teleportation equation* (which catches main features of quantum teleportation and is defined in the next section) in terms of the unitary braid representation b -matrix, and suggest *the braid teleportation* $(b^{-1} \otimes Id)(Id \otimes b)$ with identity Id to describe quantum teleportation. We present an interpretation for the braid teleportation in view of the crossed measurement [37, 38, 39], and explore the configuration for the braid teleportation in the state model [10] (which is devised for the braid representation of the TL algebra). Furthermore, the virtual braid group [40] is an extension of the braid group by the symmetric group, and it has virtual crossings acting like permutation P . We suggest *the teleportation swapping* $(P \otimes Id)(Id \otimes P)$ as a special example of the braid teleportation. The virtual mixed relation for defining the virtual braid group is found to be a reformulation of the teleportation equation, which leads to our suggestion of *the virtual braid teleportation*. Moreover, similar to the braid representation of the TL algebra [10], the virtual braid representation can be constructed in terms of the Brauer algebra [41] (or the virtual TL algebra [31, 42]). The Temperley–Lieb configuration for quantum teleportation can be recognized as a fundamental configuration defining the diagrammatical Brauer algebra.

The maximally bipartite entangled pure state is a projector, and is able to form a representation of the TL algebra. Based on the diagrammatical representation for the TL algebra (i.e., configurations in terms of cups and caps [10]), we devise *the extended TL diagrammatical rules* to explore topological-like features in quantum circuits (or quantum information protocols) involving maximally bipartite entangled

states and local unitary transformations, for examples, quantum teleportation, entanglement swapping, universal quantum computation, quantum information flow, and etc. A maximally entangled Dirac ket (bra) is represented by a configuration of a cup (cap), and a local unitary transformation (its adjoint) is denoted by a solid point (a small circle). In our extended TL diagrammatical framework, various approaches to quantum teleportation have a unified diagrammatical description, and they include its standard description [8, 9], the transfer operator (or quantum information flow) [43], measurement-based quantum teleportation [38], and Werner's tight teleportation schemes [30]. The transfer operator is described by a configuration involving a top cap and a bottom cup in which the teleportation appears to be a kind of the flow of quantum information. The measurement-based quantum teleportation has a typical TL configuration as a product of generators of the TL algebra, and this diagram is able to describe both discrete and continuous quantum teleportation schemes. The diagram describing the tight teleportation scheme is a closure of the configuration for measurement-based quantum teleportation, and it naturally derives a characteristic equation for quantum teleportation since a closed configuration in the extended TL diagrammatical rules corresponds to a trace of products of operators.

The extended TL diagrammatical rules present a diagrammatical representation of *the extended TL algebra* as an extension of the TL algebra by local unitary transformations. The collection of all the extended TL algebras is called *the extended TL category* [32, 33, 34], and its diagrammatical representation includes all configurations made of cups, caps, solid points and small circles. Besides its application to quantum teleportation, it is able to describe entanglement swapping [44], universal quantum computation [45], and etc. Entanglement swapping is an approach to producing an entangled state between two independent systems via quantum measurements, and the closure of its diagrammatical description gives rise to the tight entanglement swapping scheme with a characteristic equation. Universal quantum computation is performed in the extended TL category, since we are able to construct unitary braid gates, the swap gate and CNOT gate, etc., with the extended TL diagrammatical rules. Furthermore, we recognize another equivalent description of quantum teleportation in terms of the swap gate and Bell measurements, after identifying the configuration for quantum teleportation with that for the axiom of the Brauer algebra [31, 42]. Moreover, we comment on multipartite entanglements in the extended TL diagrammatical approach.

Quantum teleportation can be viewed as a flow of quantum information from the sender to the receiver, and hence quantum information flow can be well described in the extended TL diagrammatical framework. In its configuration, the flow is only a part of the entire diagram, related to or even controlled by other parts. For example, it is zero due to the vanishing trace of a product of local unitary transformations which are not involved in the flow. Besides our diagrammatical approach, quantum information flow has been described by Kauffman's teleportation topology [13, 29] and Abramsky and Coecke's strongly compact closed categories [46]. There are essential physical and mathematical differences among them. Measurement-based quantum teleportation is chosen to present a full description of quantum teleportation in our study, whereas quantum information flow denoted by the transfer operator is regarded as the entire quantum teleportation in both [13, 29] and [46]. We show that the paradigm described by the transfer operator is

a part of the picture by measurement-based quantum teleportation. Furthermore, only topological-like features [34] can be explored in the extended TL diagrammatical configuration instead of pure topology in [13, 29]. Moreover, we propose the extended TL category underlying quantum information protocols like quantum teleportation instead of strongly compact closed categories, see [34] for more details.

The plan of this paper is organized as follows. Section 2 introduces the teleportation equation and reformulates it respectively by the braid group, the symmetric group and the virtual braid group. Section 3-7 introduces the extended TL diagrammatical approach to quantum information and computation: Section 3 explains diagrammatical rules with examples; Section 4 unifies various descriptions of quantum teleportation at the diagrammatical level; Section 5 focuses on the TL algebra and the Brauer algebra; Section 6 deals with the entanglement swapping and universal quantum computation; Section 7 compares the quantum information flow in the extended TL category with other known approaches. Last section comments on our work in the project of setting up categorical foundations for quantum physics and information.

2. Braid teleportation, teleportation swapping and virtual braid teleportation

We describe quantum teleportation in the language of the braid group, the symmetric group, and the virtual braid group, respectively, and propose the braid teleportation, the teleportation swapping, and the virtual braid teleportation. First of all, we revisit the standard description of the teleportation [8, 9] and assign the name *the teleportation equation* to its most important equality. Secondly, we reformulate the teleportation equation in terms of the Bell matrix which forms a unitary braid representation, and then realize that a braiding operator called *the braid teleportation* plays a key role in the formulation of the teleportation equation. Thirdly, we discuss *the teleportation swapping* as a simplest example of the braid teleportation, and recognize the teleportation equation as a reformulation of the virtual mixed relation defining the virtual braid group. Lastly, we look upon the braid teleportation as a kind of crossed measurement if it has a sort of physical correspondence, and expand it in the state model [10] which sheds an insight on the main topic in the following sections.

2.1. Quantum teleportation: the teleportation equation. The Pauli matrices σ_1 , σ_2 and σ_3 have the conventional form,

$$(1) \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and quantum states $|0\rangle$ and $|1\rangle$ as a basis denoting a qubit have the coordinate presentation in the complex field \mathbb{C} ,

$$(2) \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

which give rise to useful formulas: $a, b \in \mathbb{C}$,

$$(3) \quad \sigma_1 \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}, \quad -i\sigma_2 \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -b \\ a \end{pmatrix}, \quad \sigma_3 \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix}.$$

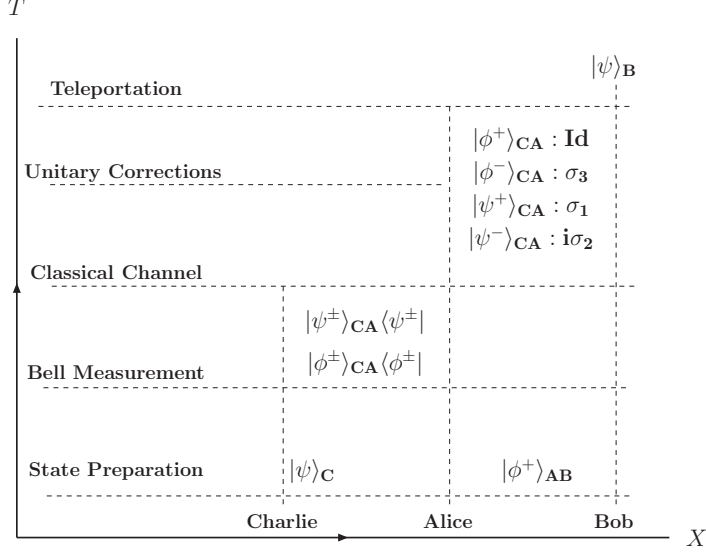


FIGURE 1. Diagrammatical description of quantum teleportation.

The product basis of two-fold tensor products denoting two-qubit is chosen to be

$$(4) \quad |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

which fixes our rule for calculating the tensor product of matrices, i.e., embedding the right matrix into the left one. With the product basis $|ij\rangle$, $i, j = 0, 1$, four mutually orthogonal Bell states have the form,

$$(5) \quad \begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), & |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \end{aligned}$$

which derive the product basis $|ij\rangle$ in terms of Bell states,

$$(6) \quad \begin{aligned} |00\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle), & |01\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle), \\ |10\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle), & |11\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle). \end{aligned}$$

Bell states can be transformed to each other with local unitary transformations consisting of Pauli matrices and identity matrix \mathbb{I}_2 ,

$$(7) \quad \begin{aligned} |\phi^-\rangle &= (\mathbb{I}_2 \otimes \sigma_3)|\phi^+\rangle = (\sigma_3 \otimes \mathbb{I}_2)|\phi^+\rangle, \\ |\psi^+\rangle &= (\mathbb{I}_2 \otimes \sigma_1)|\phi^+\rangle = (\sigma_1 \otimes \mathbb{I}_2)|\phi^+\rangle, \\ |\psi^-\rangle &= (\mathbb{I}_2 \otimes -i\sigma_2)|\phi^+\rangle = (i\sigma_2 \otimes \mathbb{I}_2)|\phi^+\rangle, \end{aligned}$$

where one-qubit unitary transformations are called local unitary transformations.

Quantum teleportation transports a unknown quantum state $|\psi\rangle_C = (a|0\rangle + b|1\rangle)_C$ from the sender, Charlie to the receiver, Bob, with the help of Alice, and it exploits properties of quantum entanglement and quantum measurement. Figure 1 is our diagrammatical interpretation for quantum teleportation. Let Alice and Bob share the Bell state $|\phi^+\rangle_{AB}$, a maximally bipartite entangled pure state. Do calculation:

$$\begin{aligned}
 |\psi\rangle_C |\phi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(a|0\rangle + b|1\rangle)_C(|00\rangle + |11\rangle)_{AB} \\
 &= \frac{1}{2}a(|\phi^+\rangle + |\phi^-\rangle)_{CA}|0\rangle_B + \frac{1}{2}a(|\psi^+\rangle + |\psi^-\rangle)_{CA}|1\rangle_B \\
 &\quad + \frac{1}{2}b(|\psi^+\rangle - |\psi^-\rangle)_{CA}|0\rangle_B + \frac{1}{2}b(|\phi^+\rangle - |\phi^-\rangle)_{CA}|1\rangle_B \\
 (8) \quad &= \frac{1}{2}(|\phi^+\rangle_{CA}|\psi\rangle_B + |\phi^-\rangle_{CA}\sigma_3|\psi\rangle_B + |\psi^+\rangle_{CA}\sigma_1|\psi\rangle_B + |\psi^-\rangle_{CA}(-i\sigma_2)|\psi\rangle_B)
 \end{aligned}$$

which is an identity but called *the teleportation equation* in our research for convenience. Alice performs Bell measurements in the composite system of Charlie and her, and obtains four kinds of outcomes. After Alice detects the Bell state $|\phi^+\rangle_{CA}$ and informs it to Bob through a classical channel, Bob knows that he has the quantum state $|\psi\rangle_B$ which Charlie wants to send to him. As Alice gets Bell states $|\phi^-\rangle_{CA}$ or $|\psi^+\rangle_{CA}$ or $|\psi^-\rangle_{CA}$, Bob applies local unitary transformations σ_3 or σ_1 or $i\sigma_2$ respectively, on the quantum state that he has to obtain $|\psi\rangle_B$.

There exist beautiful mathematical structures underlying quantum teleportation, though only fundamental laws of quantum mechanics and a little linear algebra are involved in its standard description. In this paper, we make it clear that quantum teleportation can be described by the braid group, the symmetric group, the virtual braid group, the TL algebra and the Brauer algebra.

2.2. Teleportation equation in terms of Bell matrix. Let us introduce the Bell matrix [13, 17, 12], denoted by $B = (B_{ij,lm})$, $i, j, l, m = 0, 1$. As a unitary transformation matrix from the product basis to the basis formed by Bell states, it forms a unitary braid representation as well as a universal quantum gate in universal quantum computation. The B matrix and its inverse B^{-1} (or transpose B^T) have the form

$$(9) \quad B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}, \quad B^{-1} = B^T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

It has an exponential formalism given by

$$(10) \quad B = e^{i\frac{\pi}{4}(\sigma_1 \otimes \sigma_2)} = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4}(\sigma_1 \otimes \sigma_2)$$

with interesting properties:

$$(11) \quad B^2 = i\sigma_1 \otimes \sigma_2, \quad B^4 = -\mathbb{1}_4, \quad B^8 = \mathbb{1}_4, \quad B = \frac{1}{\sqrt{2}}(\mathbb{1}_4 + B^2).$$

In terms of the B matrix and product basis $|ij\rangle$, Bell states is yielded in two ways:

$$\begin{aligned}
 (I) : \quad & |\phi^+\rangle = B|11\rangle, & |\phi^-\rangle &= B|00\rangle, \\
 (12) \quad & |\psi^+\rangle = B|01\rangle, & |\psi^-\rangle &= -B|10\rangle,
 \end{aligned}$$

and

$$(II) : \quad \begin{aligned} |\phi^+\rangle &= B^T|00\rangle, & |\phi^-\rangle &= -B^T|11\rangle, \\ |\psi^+\rangle &= B^T|10\rangle, & |\psi^-\rangle &= B^T|01\rangle, \end{aligned} \quad (13)$$

where the Bell operator B acts on the basis $|ij\rangle$ in the way

$$B|ij\rangle = \sum_{k,l=0}^1 |kl\rangle B_{kl,ij} = \sum_{k,l=0}^1 |kl\rangle B_{ij,kl}^T. \quad (14)$$

For simplicity, we exploit the first type of transformation law (I) between Bell states and the product basis, and rewrite the teleportation equation (8) into a new formalism,

$$\begin{aligned} & (\mathbb{1}_2 \otimes B)(|\psi\rangle \otimes |11\rangle)_{CAB} \\ &= \frac{1}{2}(B \otimes \mathbb{1}_2)(|00\rangle \otimes \sigma_3|\psi\rangle + |01\rangle \otimes \sigma_1|\psi\rangle + |10\rangle \otimes i\sigma_2|\psi\rangle + |11\rangle \otimes |\psi\rangle)_{CAB}, \\ (15) \quad & \equiv (B \otimes \mathbb{1}_2)(\vec{v}^T \otimes \frac{1}{2}\vec{\sigma}_{11}|\psi\rangle)_{CAB} \end{aligned}$$

in which the vector \vec{v} , its transpose given by

$$(16) \quad \vec{v}^T = (|00\rangle, |01\rangle, |10\rangle, |11\rangle), \quad v_{ij} = |ij\rangle, \quad i, j = 0, 1,$$

the vector $\vec{\sigma}_{11}$, its transpose given by

$$(17) \quad \vec{\sigma}_{11}^T = (\sigma_3, \sigma_1, i\sigma_2, \mathbb{1}_2),$$

and the calculation of $\vec{v}^T \otimes \vec{\sigma}_{11}$ follows the rule,

$$(18) \quad \vec{v}^T \otimes \vec{\sigma}_{11}|\psi\rangle \equiv |00\rangle \otimes \sigma_3|\psi\rangle + |01\rangle \otimes \sigma_1|\psi\rangle + |10\rangle \otimes i\sigma_2|\psi\rangle + |11\rangle \otimes |\psi\rangle.$$

The remaining three teleportation equations are derived in a similar way with the help of local unitary transformations among Bell states (7). For example,

$$\begin{aligned} & |\psi\rangle_C |\phi^-\rangle_{AB} = (\mathbb{1}_2 \otimes B)(|\psi\rangle \otimes |00\rangle)_{CAB} \\ &= |\psi\rangle_C \otimes (\mathbb{1}_2 \otimes \sigma_3)|\phi^+\rangle_{AB} = (\mathbb{1}_2 \otimes \mathbb{1}_2 \otimes \sigma_3)|\psi\rangle_C |\phi^+\rangle_{AB} \\ (19) \quad &= (B \otimes \mathbb{1}_2)(\vec{v}^T \otimes \frac{1}{2}\sigma_3\vec{\sigma}_{11}|\psi\rangle)_{CAB} \end{aligned}$$

where the local unitary transformation $\mathbb{1}_2 \otimes \mathbb{1}_2 \otimes \sigma_3$ commutes with $B \otimes \mathbb{1}_2$, and the other two teleportation equations have the form,

$$\begin{aligned} & (\mathbb{1}_2 \otimes B)(|\psi\rangle \otimes |01\rangle)_{CAB} = (B \otimes \mathbb{1}_2)(\vec{v}^T \otimes \frac{1}{2}\sigma_1\vec{\sigma}_{11}|\psi\rangle)_{CAB}, \\ (20) \quad & (\mathbb{1}_2 \otimes B)(|\psi\rangle \otimes -|10\rangle)_{CAB} = (B \otimes \mathbb{1}_2)(\vec{v}^T \otimes -\frac{1}{2}i\sigma_2\vec{\sigma}_{11}|\psi\rangle)_{CAB}. \end{aligned}$$

These four teleportation equations can be collected into an equation,

$$\begin{aligned} & (\mathbb{1}_2 \otimes B)(|\psi\rangle \otimes \vec{v}^T)_{CAB} = (B \otimes \mathbb{1}_2)(\vec{v}^T \otimes \frac{1}{2}\vec{\Sigma}|\psi\rangle)_{CAB}, \\ (21) \quad & (\vec{v}^T \otimes \frac{1}{2}\vec{\Sigma}|\psi\rangle)_{CAB} = (B^{-1} \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B)(|\psi\rangle \otimes \vec{v}^T)_{CAB}, \end{aligned}$$

in terms of the new matrix $\vec{\Sigma}$, a convenient notation given by

$$(22) \quad \vec{\Sigma} = (\sigma_3, \sigma_2, i\sigma_1, \mathbb{1}_2)\vec{\sigma}_{11}$$

where $\vec{v}^T \otimes \vec{\Sigma}$ is defined as

$$(23) \quad \vec{v}^T \otimes \vec{\Sigma}|\psi\rangle \equiv (\vec{v}^T \otimes \sigma_3 \vec{\sigma}_{11}|\psi\rangle, \vec{v}^T \otimes \sigma_2 \vec{\sigma}_{11}|\psi\rangle, \vec{v}^T \otimes i\sigma_1 \vec{\sigma}_{11}|\psi\rangle, \vec{v}^T \otimes \vec{\sigma}_{11}|\psi\rangle),$$

and $|\psi\rangle \otimes \vec{v}^T$ has the form

$$(24) \quad |\psi\rangle \otimes \vec{v}^T \equiv (|\psi\rangle \otimes |00\rangle, |\psi\rangle \otimes |01\rangle, |\psi\rangle \otimes |10\rangle, |\psi\rangle \otimes |11\rangle).$$

Obviously, the operator $(B^{-1} \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B)$ plays a fundamental role in the new formulations of the teleportation equation. In the following, we verify the Bell matrix B a unitary braid representation, and then name the braiding operator of this kind as *the braid teleportation*.

2.3. Braid teleportation and teleportation swapping. A braid representation b -matrix is a $d \times d$ matrix acting on $V \otimes V$ where V is an d -dimensional vector space over the complex field \mathbb{C} . The symbol b_i denotes the braid b acting on the tensor product $V_i \otimes V_{i+1}$. The classical braid group B_n is generated by braids b_1, b_2, \dots, b_{n-1} satisfying the braid group relation,

$$(25) \quad \begin{aligned} b_i b_j &= b_j b_i, & j &\neq i \pm 1, \\ b_i b_{i+1} b_i &= b_{i+1} b_i b_{i+1}, & i &= 1, \dots, n-2. \end{aligned}$$

The virtual braid group VB_n is an extension of the classical braid group B_n by the symmetric group S_n [40]. It has two types of generators: braids b_i and virtual crossings v_i defined by the virtual crossing relation,

$$(26) \quad \begin{aligned} v_i^2 &= Id, & v_i v_{i+1} v_i &= v_{i+1} v_i v_{i+1}, & i &= 1, \dots, n-2, \\ v_i v_j &= v_j v_i, & j &\neq i \pm 1, \end{aligned}$$

a presentation of the symmetric group S_n with identity Id , and they satisfying the virtual mixed relation,

$$(27) \quad \begin{aligned} b_i v_j &= v_j b_i, & j &\neq i \pm 1, \\ b_{i+1} v_i v_{i+1} &= v_i v_{i+1} b_i, & i &= 1, \dots, n-2. \end{aligned}$$

The Bell matrix B forms a unitary braid representation. After some algebra, the right handside of the braid group relation (25) has a form

$$(28) \quad \begin{aligned} &(\mathbb{1}_2 \otimes B)(B \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B) \\ &= \frac{1}{2\sqrt{2}}(\mathbb{1}_8 + \mathbb{1}_2 \otimes i\sigma_1 \otimes \sigma_2)(\mathbb{1}_8 + i\sigma_1 \otimes \sigma_2 \otimes \mathbb{1}_2)(\mathbb{1}_8 + \mathbb{1}_2 \otimes i\sigma_1 \otimes \sigma_2) \\ &= \frac{i}{\sqrt{2}}(\mathbb{1}_2 \otimes \sigma_1 \otimes \sigma_2 + \sigma_1 \otimes \sigma_2 \otimes \mathbb{1}_2) = \frac{1}{\sqrt{2}}(\mathbb{1}_2 \otimes B^2 + B^2 \otimes \mathbb{1}_2) \end{aligned}$$

and its left handside leads to the same result,

$$(29) \quad (B \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B)(B \otimes \mathbb{1}_2) = \frac{1}{\sqrt{2}}(\mathbb{1}_2 \otimes B^2 + B^2 \otimes \mathbb{1}_2).$$

Furthermore, the Bell matrix B as a classical crossing and the permutation matrix P as a virtual crossing,

$$(30) \quad P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad P|ij\rangle = |ji\rangle, \quad i, j = 0, 1,$$

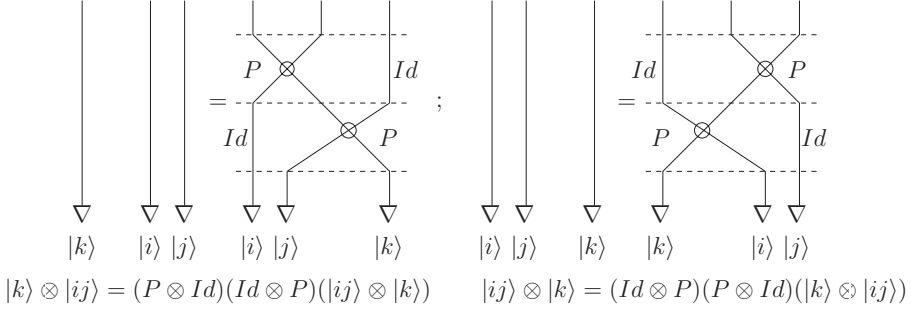


FIGURE 2. Teleportation swapping.

form a unitary virtual braid representation. The left handside of the virtual mixed relation (27) has a form

$$(31) \quad (\mathbb{1}_2 \otimes B)(P \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P)(|i\rangle \otimes |j\rangle \otimes |k\rangle) = (\mathbb{1}_2 \otimes B)(|k\rangle \otimes |ij\rangle),$$

while its right handside leads to the form

$$(32) \quad \begin{aligned} & (P \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P)(B \otimes \mathbb{1}_2)(|i\rangle \otimes |j\rangle \otimes |k\rangle) \\ &= \sum_{k,l=0}^1 B_{i'j',ij}(P \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P)(|i'j'\rangle \otimes |k\rangle) \\ &= \sum_{k,l=0}^1 B_{i'j',ij}(|k\rangle \otimes |i'j'\rangle) = (\mathbb{1}_2 \otimes B)(|k\rangle \otimes |ij\rangle). \end{aligned}$$

Here we suggest the unitary braiding operator $(b^{-1} \otimes Id)(Id \otimes b)$ as the braid teleportation underlying quantum teleportation. Its simplest example $(P \otimes Id)(Id \otimes P)$ is called the teleportation swapping in view of the fact that the braid group (25) is a generation of of the symmetric group (26), and it has the other example $(B^{-1} \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B)$ in terms of the Bell matrix. There are two natural teleportation swapping operators $(P \otimes Id)(Id \otimes P)$ and $(Id \otimes P)(P \otimes Id)$ in terms of the permutation operator P , satisfying the following teleportation swapping equalities,

$$(33) \quad \begin{aligned} |k\rangle \otimes |ij\rangle &= (P \otimes Id)(Id \otimes P)(|ij\rangle \otimes |k\rangle), \\ |ij\rangle \otimes |k\rangle &= (Id \otimes P)(P \otimes Id)(|k\rangle \otimes |ij\rangle), \end{aligned}$$

which are shown in Figure 2, the virtual crossing P denoted by a cross with a small circle.

2.4. Virtual braid teleportation. Let us describe quantum teleportation in the language of the virtual braid group. The braid group relation (25) represents a connection between topological entanglements and quantum entanglements, while the virtual mixed relation (27) is a reformulation of the teleportation equation (8). A nontrivial unitary braid detecting knots or links can be often identified with a universal quantum gate transforming a separate state into an entangled one, see [13, 17, 18], and it acts as a device yielding an entangled source. On the other hand, the teleportation swapping in terms of a virtual crossings v_i is responsible for quantum teleportation. In the following, the virtual mixed relation (27) is shown as a reformulation of the teleportation equation (8).

Note that the permutation matrix P has a form

$$(34) \quad P = \frac{1}{2}(\mathbb{1}_4 + \sigma_1 \otimes \sigma_1 + \sigma_2 \otimes \sigma_2 + \sigma_3 \otimes \sigma_3),$$

and local unitary transformations (7) among Bell states are given by

$$(35) \quad \begin{aligned} |\phi^-\rangle &= B|00\rangle = (\mathbb{1}_2 \otimes \sigma_3)B|11\rangle = (\sigma_3 \otimes \mathbb{1}_2)B|11\rangle, \\ |\psi^+\rangle &= B|01\rangle = (\mathbb{1}_2 \otimes \sigma_1)B|11\rangle = (\sigma_1 \otimes \mathbb{1}_2)B|11\rangle, \\ |\psi^-\rangle &= -B|10\rangle = (\mathbb{1}_2 \otimes -i\sigma_2)B|11\rangle = (i\sigma_2 \otimes \mathbb{1}_2)B|11\rangle. \end{aligned}$$

In terms of the Bell matrix and teleportation swapping, the left handside of the teleportation equation (8) has a form,

$$(36) \quad \begin{aligned} |\psi\rangle_C \otimes |\phi^+\rangle_{AB} &= (\mathbb{1}_2 \otimes B)(|\psi\rangle_C \otimes |11\rangle_{AB}) \\ &= (\mathbb{1}_2 \otimes B)(P \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P)(|11\rangle_{CA} \otimes |\psi\rangle_B), \end{aligned}$$

while its right handside leads to the other form,

$$(37) \quad \begin{aligned} &\frac{1}{2}(|\phi^-\rangle_{CA}\sigma_3|\psi\rangle_B + |\psi^-\rangle_{CA}(-i\sigma_2)|\psi\rangle_B + |\psi^+\rangle_{CA}\sigma_1|\psi\rangle_B + |\phi^+\rangle_{CA}|\psi\rangle_B) \\ &= \frac{1}{2}(\mathbb{1}_2 \otimes \sigma_3 \otimes \sigma_3 + \mathbb{1}_2 \otimes i\sigma_2 \otimes i\sigma_2 + \mathbb{1}_2 \otimes \sigma_1 \otimes \sigma_1 + \mathbb{1}_8)(B \otimes \mathbb{1}_2)(|11\rangle_{CA} \otimes |\psi\rangle_B) \\ &= (\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_2 \otimes \sigma_2)(B \otimes \mathbb{1}_2)(|11\rangle_{CA} \otimes |\psi\rangle_B) \end{aligned}$$

Hence the teleportation equation (8) can be recognized to be either a kind of the teleportation swapping,

$$(38) \quad \begin{aligned} |\psi\rangle_C \otimes |\phi^+\rangle_{AB} &= (\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_2 \otimes \sigma_2)(|\phi^+\rangle_{CA} \otimes |\psi\rangle_B) \\ &= (P \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P)(|\phi^+\rangle_{CA} \otimes |\psi\rangle_B), \end{aligned}$$

or a reformulation of the virtual mixed relation (27),

$$(39) \quad \begin{aligned} &(\mathbb{1}_2 \otimes B)(P \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P)(|11\rangle_{CA} \otimes |\psi\rangle_B) \\ &= (\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_2 \otimes \sigma_2)(B \otimes \mathbb{1}_2)(|11\rangle_{CA} \otimes |\psi\rangle_B) \\ &= (P \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P)(B \otimes \mathbb{1}_2)(|11\rangle_{CA} \otimes |\psi\rangle_B). \end{aligned}$$

The remaining three teleportation equations can be reformulated by applying local unitary transformations to the teleportation equation (38). The teleportation equation for the Bell state $|\phi^-\rangle_{AB}$ is obtained to be

$$(40) \quad \begin{aligned} &|\psi\rangle_C \otimes |\phi^-\rangle_{AB} = (\mathbb{1}_2 \otimes \sigma_3 \otimes \mathbb{1}_2)(|\psi\rangle_C \otimes |\phi^+\rangle_{AB}) \\ &= (\mathbb{1}_2 \otimes \sigma_3 \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_2 \otimes \sigma_2)(\mathbb{1}_2 \otimes \sigma_3 \otimes \mathbb{1}_2)(|\phi^-\rangle_{CA} \otimes |\psi\rangle_B) \\ &= (\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_1 \otimes \sigma_1)(|\phi^-\rangle_{CA} \otimes |\psi\rangle_B), \end{aligned}$$

and the teleportation equations for Bell states $|\psi^\pm\rangle_{AB}$ have the form,

$$(41) \quad \begin{aligned} &|\psi\rangle_C \otimes |\psi^+\rangle_{AB} = (\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_3 \otimes \sigma_3)(|\psi^+\rangle_{CA} \otimes |\psi\rangle_B), \\ &|\psi\rangle_C \otimes |\psi^-\rangle_{AB} = (\mathbb{1}_2 \otimes P - \mathbb{1}_8)(|\psi^-\rangle_{CA} \otimes |\psi\rangle_B), \end{aligned}$$

in which local unitary transformations of $(\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_2 \otimes \sigma_2)$ are exploited,

$$(42) \quad \begin{aligned} &(\mathbb{1}_2 \otimes \sigma_1 \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_2 \otimes \sigma_2)(\mathbb{1}_2 \otimes \sigma_1 \otimes \mathbb{1}_2) = \mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_3 \otimes \sigma_3, \\ &(\mathbb{1}_2 \otimes i\sigma_2 \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes P - \mathbb{1}_2 \otimes \sigma_2 \otimes \sigma_2)(\mathbb{1}_2 \otimes i\sigma_2 \otimes \mathbb{1}_2) = \mathbb{1}_2 \otimes P - \mathbb{1}_8. \end{aligned}$$

As a remark, a unitary braid is a device of entangling separate states in the virtual braid teleportation, whereas a unitary braiding operator plays a role of quantum teleportation in the braid teleportation.

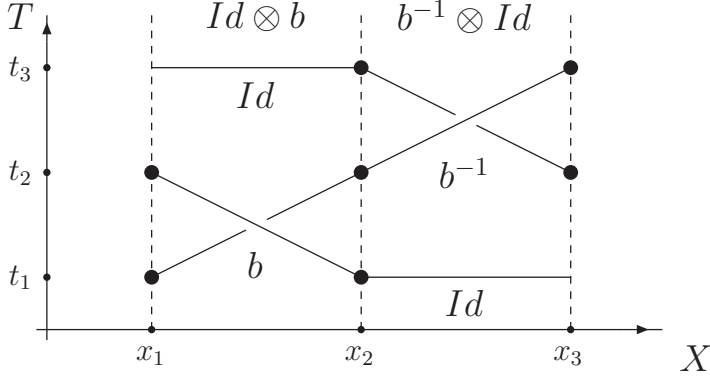


FIGURE 3. Braid teleportation using the crossed measurement.

$$b = \begin{array}{c} \diagup \\ \diagdown \end{array} = A \left| \begin{array}{c} \diagup \\ \diagdown \end{array} \right| + A^{-1} \left| \begin{array}{c} \diagdown \\ \diagup \end{array} \right| ; \quad b^{-1} = \begin{array}{c} \diagdown \\ \diagup \end{array} = A^{-1} \left| \begin{array}{c} \diagup \\ \diagdown \end{array} \right| + A \left| \begin{array}{c} \diagdown \\ \diagup \end{array} \right|$$

 FIGURE 4. Braid b and its inverse b^{-1} in the state model.

2.5. Braid teleportation, crossed measurement and state model. We explore the braid teleportation, ie., a unitary braiding operator $(b^{-1} \otimes Id)(Id \otimes b)$, from both physical and mathematical perspectives. In view of Vaidman's crossed measurement [37], a unitary braid or crossing acts as a device of non-local measurement in space-time. In Figure 3, two lines of the crossing b represent two observable operations: the first one relating quantum measurement at the space-time point (x_1, t_1) to that at the other point (x_2, t_2) and the second one relating quantum measurement at (x_1, t_2) to that at (x_2, t_1) . The crossed measurement $(Id \otimes b)$ plays the role of sending a qubit (with a possible local unitary transformation) from Charlie to Alice. Similarly, the crossed measurement $(b^{-1} \otimes Id)$ transfers the qubit from Alice to Bob with a possible local unitary transformation. Note that this kind of interpretation for a unitary braiding operator is not the same as the braid statistics of anyons [47].

Furthermore, the braid teleportation $(b^{-1} \otimes Id)(Id \otimes b)$ is different from $(Id \otimes b)(b^{-1} \otimes Id)$, namely, two crossed measurements are not commutative with each other. For example, we rewrite the Bell teleportation $(B^{-1} \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B)$ into the other formalism,

$$\begin{aligned} (B^{-1} \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B) &= \frac{1}{2}((\mathbb{1}_4 - B^2) \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes (\mathbb{1}_4 + B^2)) \\ &= \frac{1}{2}(\mathbb{1}_2 \otimes (\mathbb{1}_4 + B^2))((\mathbb{1}_4 - B^2) \otimes \mathbb{1}_2) + (\mathbb{1}_2 \otimes B^2)(B^2 \otimes \mathbb{1}_2) \\ (43) \quad &= (\mathbb{1}_2 \otimes B)(B^{-1} \otimes \mathbb{1}_2) + (\mathbb{1}_2 \otimes B^2)(B^2 \otimes \mathbb{1}_2) \end{aligned}$$

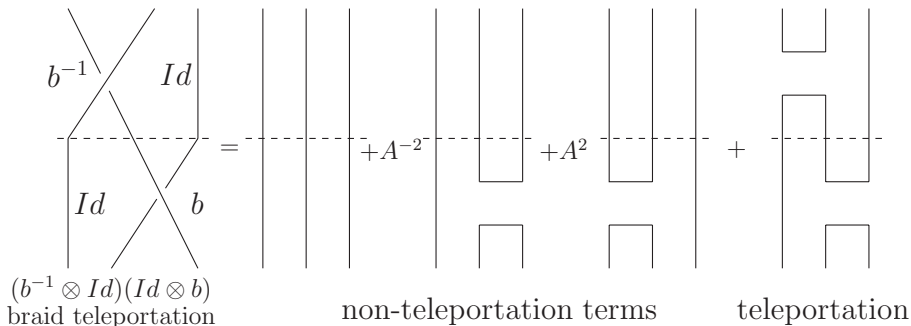


FIGURE 5. Braid teleportation in the state model.

where we exploit

$$(44) \quad (\mathbb{1}_2 \otimes B^2)(B^2 \otimes \mathbb{1}_2) = -(B^2 \otimes \mathbb{1}_2)(\mathbb{1}_2 \otimes B).$$

and B^2 does not form a braid representation.

Moreover, we explore the configuration for the braid teleportation $(b^{-1} \otimes Id)(Id \otimes b)$ in the state model for knot theory [10]. It is an approach to a disentanglement of a knot or link, see Figure 4. A braid b is denoted by a under-crossing and its inverse b^{-1} is denoted by an over-crossing. Each crossing is identified with a linear combination of two types of configurations: the first given by two straight lines representing identity and the second given by a top cup together with a bottom cap representing a projector. The coefficients A, A^{-1} are specified by which state model to be used [10]. In Figure 5, the braid teleportation has four diagrammatical terms. A part above a dashed line is contributed from $(b^{-1} \otimes Id)$ and a part under the dashed line is from $(Id \otimes b)$. Obviously, the first three are irrelevant with quantum teleportation but the fourth one takes charge for it.

As a remark, the state model for knot theory [10] is a diagrammatical recipe for the braid representation of the TL algebra, and the teleportation term in Figure 5 is a typical configuration in the diagrammatical TL algebra. In the following, we focus on the topic how the TL algebra with local unitary transformations describes quantum information and computation.

3. Extended TL diagrammatical approach (I): diagrammatical rules and examples

In the following sections from Section 3 to Section 7, we propose the extended Temperley–Lieb diagrammatical approach and exploit it to study various topics in quantum information and computation. In this section, we devise the extended TL diagrammatical rules and explain them by examples.

3.1. Maximally entangled bipartite pure states. Maximally entangled bipartite pure states play key roles in quantum information and computation, and how to make a diagrammatical representation for them is a bone of the extended TL diagrammatical rules.

The vectors $|e_i\rangle$, $i = 0, 1, \dots, d-1$ form an orthogonal basis in a d -dimension Hilbert space \mathcal{H} and the covectors $\langle e_i|$, are chosen in its dual Hilbert space \mathcal{H}^* ,

$$(45) \quad \sum_{i=0}^{d-1} |e_i\rangle\langle e_i| = \mathbb{1}_d, \quad \langle e_j|e_i\rangle = \delta_{ij}, \quad i, j = 0, 1, \dots, d-1,$$

where δ_{ij} is the Kronecker symbol and $\mathbb{1}_d$ denotes a d -dimensional identity matrix. The maximally entangled state $|\Omega\rangle$, a quantum state in the two-fold tensor product $\mathcal{H} \otimes \mathcal{H}$ of the Hilbert space \mathcal{H} , and its dual state $\langle\Omega|$ are respectively given by

$$(46) \quad |\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i \otimes e_i\rangle, \quad \langle\Omega| = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} \langle e_i \otimes e_i|,$$

The local action of a bounded linear operator M in the Hilbert space \mathcal{H} on $|\Omega\rangle$ satisfies

$$(47) \quad \begin{aligned} |\psi\rangle &\equiv (M \otimes \mathbb{1}_d)|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} M|e_i\rangle \otimes |e_i\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} |e_j\rangle M_{ji} \otimes |e_i\rangle = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} |e_j\rangle \otimes |e_i\rangle M_{ij}^T \\ &= (\mathbb{1}_d \otimes M^T)|\Omega\rangle, \quad M_{ij} = \langle e_i|M|e_j\rangle, \quad M_{ij}^T = M_{ji}, \end{aligned}$$

where the upper index T denotes the transpose, and hence it is permitted to move a local action of the operator M in the Hilbert space to the other Hilbert space if it acts on $|\Omega\rangle$. A trace of two operators M^\dagger and M' can be represented by an inner product between $|\psi\rangle$ and $|\psi'\rangle$,

$$(48) \quad \begin{aligned} \langle\psi|\psi'\rangle &\equiv \langle\Omega|(M^\dagger \otimes \mathbb{1}_d)(M' \otimes \mathbb{1}_d)|\Omega\rangle = \frac{1}{d} \sum_{i,j=0}^{d-1} \langle e_i|M^\dagger M'|e_j\rangle \langle e_i|e_j\rangle, \\ &= \frac{1}{d} \text{tr}(M^\dagger M'), \quad |\psi'\rangle = (M' \otimes \mathbb{1}_d)|\Omega\rangle, \end{aligned}$$

which leads to an inner product with the operator $N_1 \otimes N_2$ given by a trace,

$$(49) \quad \langle\psi|N_1 \otimes N_2|\psi'\rangle = \frac{1}{d} \text{tr}(M^\dagger N_1 M' N_2^T).$$

The transfer operator T_{BC} , sending a quantum state from Charlie to Bob, is defined by

$$(50) \quad T_{BC}|\psi\rangle_C \equiv T_{BC} \sum_{k=0}^{d-1} a_k |e_k\rangle_C = \sum_{k=0}^{d-1} a_k |e_k\rangle_B = |\psi\rangle_B,$$

and has a form of an inner product between ${}_C\langle\Omega|$ and $|\Omega\rangle_{AB}$,

$$(51) \quad \begin{aligned} {}_C\langle\Omega|\Omega\rangle_{AB} &= \frac{1}{d} \sum_{i,j=0}^{d-1} ({}_C\langle e_i| \otimes {}_A\langle e_i|)(|e_j\rangle_A \otimes |e_j\rangle_B) \\ &= \frac{1}{d} T_{BC} \equiv \frac{1}{d} \sum_{i=0}^{d-1} |e_i\rangle_B {}_C\langle e_i|, \end{aligned}$$

which is exploited by Braunstein et al. see [9].

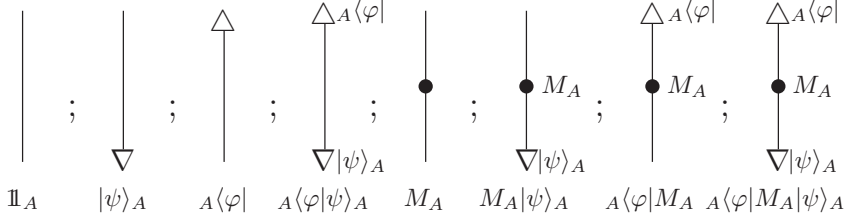


FIGURE 6. Straight lines without or with points.

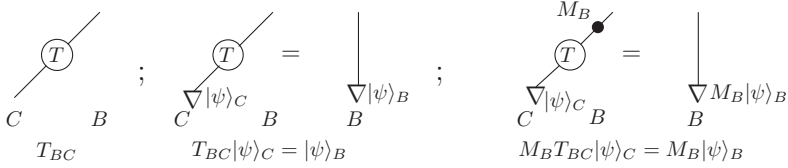


FIGURE 7. Oblique lines: the transfer operator.

A unitary transformation of $|\Omega\rangle$ is called local as the unitary operator U_n only acts on the first (or second) Hilbert space of the two-fold Hilbert space $\mathcal{H} \otimes \mathcal{H}$. The local unitary transformation of $|\Omega\rangle$ denoted by $|\Omega_n\rangle = (U_n \otimes \mathbb{1}_d)|\Omega\rangle$, is still a maximally entangled vector. The set of unitary operators U_n satisfying the orthogonal relation $\text{tr}(U_n^\dagger U_m) = d \delta_{nm}$, $n, m = 1 \cdots d^2$, forms a basis of $d \times d$ unitary matrices, where the upper index \dagger denotes the adjoint. The collection of maximally entangled states $|\Omega_n\rangle$ has the properties,

$$(52) \quad \langle \Omega_n | \Omega_m \rangle = \delta_{nm}, \quad \sum_{n=1}^{d^2} |\Omega_n\rangle \langle \Omega_n| = \mathbb{1}_{d^2}, \quad n, m = 1, \cdots d^2.$$

Introduce the symbol ω_n for the maximally entangled state $|\Omega_n\rangle \langle \Omega_n|$ and especially denote $|\Omega\rangle \langle \Omega|$ by ω , namely,

$$(53) \quad \omega \equiv |\Omega\rangle \langle \Omega|, \quad \omega_n \equiv |\Omega_n\rangle \langle \Omega_n|, \quad U_1 = \mathbb{1}_d,$$

and the set of ω_n , $n = 1, 2, \cdots d^2$ forms a set of observables over an output parameter space.

3.2. Extended TL diagrammatical rules. Three pieces of extended TL diagrammatical rules are devised for assigning a diagram to a given algebraic object. The first is our convention; the second explains what straight lines and oblique lines represent; the third describes various configurations in terms of cups and caps.

Rule 1. Read an algebraic object such as an inner product from the left-hand side to the right-hand side, and draw a diagram from the top to the bottom. Represent the operator M by a solid point, its adjoint operator M^\dagger by a small circle, its transposed operator M^T by a solid point with a cross line, and its complex conjugation operator M^* by a small circle with a cross line. Denote the Dirac ket by the symbol ∇ and the Dirac bra by the symbol Δ .

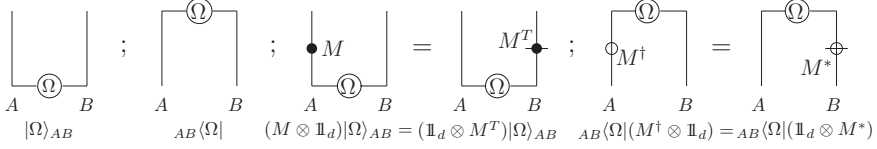


FIGURE 8. Cups and caps without or with points.

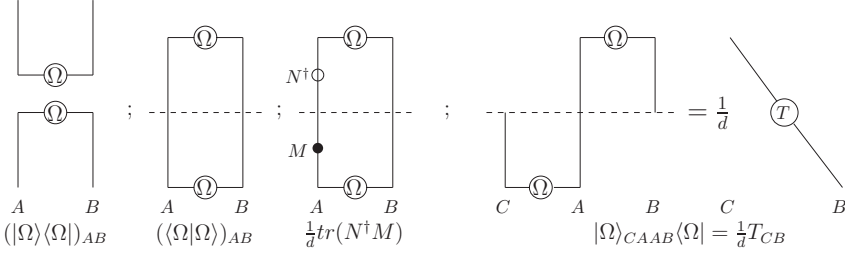


FIGURE 9. Three kinds of combinations of a cup and a cap.

Rule 2. See Figure 6. A straight line of type A denotes the identity operator $\mathbb{1}_A$ in the system A . Straight lines of type A with a bottom ∇ or top \triangle describe a vector $|\psi\rangle_A$, covector ${}_A\langle\varphi|$, and an inner product ${}_A\langle\varphi|\psi\rangle_A$ in the system A , respectively. Straight lines of type A with a middle solid point or bottom ∇ or top \triangle describe an operator M_A , a vector $M_A|\psi\rangle_A$, a covector ${}_A\langle\varphi|M_A$, and an inner product ${}_A\langle\varphi|M_A|\psi\rangle_A$, respectively.

See Figure 7. An oblique line from the system C to the system B describes the transfer operator T_{BC} , and its solid point or bottom ∇ or top \triangle have the same interpretations as those on a straight line in Figure 6.

Rule 3. See Figure 8. A cup denotes the maximally bipartite entangled state vector $|\Omega\rangle$ and a cap does for its dual $\langle\Omega|$. A cup with a middle solid point on its one branch describes a local action of the operator M on $|\Omega\rangle$, and this solid point can flow to its other branch and then is replaced by a solid point with a cross line representing M^T . The same happens for a cap except that a solid point is replaced by a small circle to distinguish the operator M from its adjoint operator M^\dagger .

A cup and a cap can form different sorts of configurations. See Figure 9. As a cup is at the top and a cap is at the bottom for the same composite system, this configuration is assigned to the projector $|\Omega\rangle\langle\Omega|$. As a cap is at the top and a cup is at the bottom for the same composite system, this diagram describes an inner product $\langle\Omega|\Omega\rangle = 1$ by a closed circle. As a cup is at the bottom for the composite system $\mathcal{H}_C \otimes \mathcal{H}_A$ and a cap is at the top for the composite system $\mathcal{H}_A \otimes \mathcal{H}_B$, that is an oblique line representing the transfer operator T_{CB} with the normalization factor $\frac{1}{d}$.

Additionally, as a cup has a local action of the operator M and a cap has a local action of the operator N^\dagger , the resulted circle with a solid point for M and a small circle for N^\dagger represents the trace $\frac{1}{d}\text{tr}(MN^\dagger)$. As a convention, we describe

FIGURE 10. The teleportation equation (8).

a trace of operators by a closed circle with solid points or small circles, and assign each cap or cup a normalization factor $\frac{1}{\sqrt{d}}$ and a circle a normalization factor d .

Note that cups and caps are well known configurations in knot theory and statistical mechanics. They were used by Wu [48] in statistical mechanics, and exploited by Kauffman [10] for diagrammatically representing the Temperley-Lieb algebra soon after Jones's work [49]. These configurations are nowadays called Brauer diagrams [41] or Kauffman diagrams [10].

3.3. Examples for the extended TL diagrammatical rules. In the following, five examples are listed as well as their corresponding algebraic counterparts to explain the extended TL diagrammatical rules in detail.

Example 1: Figure 10 is a diagrammatical representation for the teleportation equation (8). The cup denotes the Bell state $|\phi^+\rangle$, and the cups with middle solid points σ_3 , $-i\sigma_2$, σ_1 denote the Bell states $|\phi^-\rangle$, $|\psi^-\rangle$ and $|\psi^+\rangle$, respectively. The straight line with a bottom ∇ denotes a unknown state $|\psi\rangle$ to be transported, and other straight lines with middle solid points respectively denote local unitary transformations of $|\psi\rangle$.

Example 2: Figure 11 presents how to compute the inner product between $|\phi\rangle$ and $|\psi\rangle$ in the extended TL diagrammatical approach. It consists of three terms: the covector $\langle\phi|\otimes\langle\Omega|$, the local operator $\mathbb{1}_d\otimes M\otimes\mathbb{1}_d$, and the vector $|\Omega\rangle\otimes|\psi\rangle$. The vector $|\psi\rangle$ is represented by a straight line with a bottom ∇ , and the local operator $\mathbb{1}_d\otimes M\otimes\mathbb{1}_d$ is denoted by a solid point on the cup $|\Omega\rangle$. Move the local operator M from its beginning position to the other branch of the cap, change it to the local operator M^T and then allow the bottom cup and the top cap to collapse into an oblique line denoting the transfer operator with a normalization factor $\frac{1}{d}$. Besides, it can be calculated in an algebraic way

$$\begin{aligned}
 & \langle\phi\otimes\Omega|(\mathbb{1}_d\otimes M\otimes\mathbb{1}_d)|\Omega\otimes\psi\rangle \\
 &= \frac{1}{d} \sum_{i,j=0}^{d-1} \langle\phi\otimes e_i\otimes e_i|(\mathbb{1}_d\otimes M\otimes\mathbb{1}_d)|e_j\otimes e_j\otimes\psi\rangle \\
 &= \frac{1}{d} \sum_{i,j=0}^{d-1} \langle\phi|e_j\rangle\langle e_i|M|e_j\rangle\langle e_i|\psi\rangle = \frac{1}{d} \sum_{i,j=0}^{d-1} \phi_j^* M_{ji} \psi_i \\
 (54) \quad &= \frac{1}{d} \sum_{i,j=0}^{d-1} \phi_j^* M_{ji}^T \psi_i = \frac{1}{d} \langle\phi|M^T|\psi\rangle
 \end{aligned}$$

in which every step has a diagrammatical counterpart.

Example 3: Figure 12 provides a diagrammatical representation for the partial trace, which denotes the summation over a subsystem of a composite system,

$$(55) \quad \text{tr}_A(|e_i^C\rangle\langle e_j^A|\otimes|e_l^A\rangle\langle e_m^B|) = |e_i^C\rangle\langle e_m^B|\delta_{jl}, \quad \text{tr}_A(|e_j^A\rangle\langle e_l^A|) = \delta_{jl}.$$

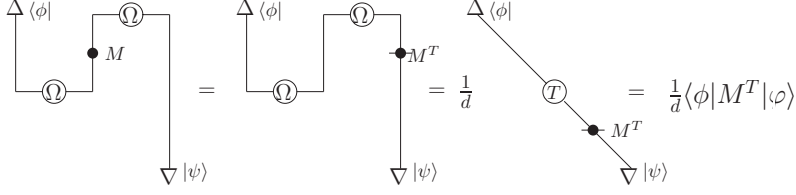


FIGURE 11. Inner product in terms of a cap and a cup.

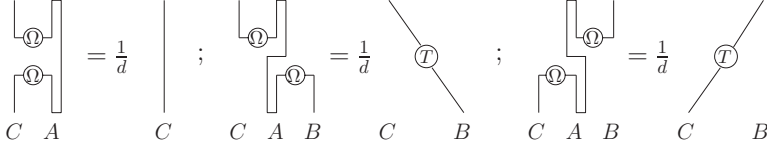


FIGURE 12. Three kinds of partial traces using a cup and a cap.

Note that the trace is a sort of partial trace, i.e., the summation over the entire composite system,

$$(56) \quad \text{tr}_{CA}(|e_i^C \otimes e_j^A\rangle\langle e_l^C \otimes e_m^A|) = \delta_{il}\delta_{jm}, \quad i, j, l, m = 0, 1, \dots, d-1.$$

The left diagrammatical term describes the one type of partial trace leading to a straight line for identity,

$$(57) \quad \text{tr}_A(|\Omega\rangle_{CA} \langle \Omega|) = \frac{1}{d} \sum_{i,j=0}^{d-1} \text{tr}_A(|e_i^C \otimes e_j^A\rangle\langle e_j^C \otimes e_i^A|) = \frac{1}{d}(\mathbb{1}_d)_C,$$

and the other two diagrammatical terms represent the other type of partial trace leading to an oblique line for the transfer operator: the middle term denotes the transfer operator T_{CB} given by

$$(58) \quad \text{tr}_A(|\Omega\rangle_{CA} \langle \Omega|) = \frac{1}{d} \sum_{i,j=0}^{d-1} \text{tr}_A(|e_i^C \otimes e_j^A\rangle\langle e_j^A \otimes e_i^B|) = \frac{1}{d}T_{CB},$$

and the right one gives rise to the transfer operator T_{CB} by

$$(59) \quad \text{tr}_A(CA \langle \Omega | \Omega \rangle_{AB}) = \frac{1}{d}T_{BC}.$$

Example 4: Figure 13 has two types of diagrams denoting the trace of operator products. In the first case, a top cup with a bottom cap forms a same closed circle as a top cap with a bottom cup, representing an algebraic equation given by

$$(60) \quad \text{tr}_{CA}((\rho_C \otimes \mathbb{1}_d |\Omega\rangle_{CA})(\langle \Omega| \mathbb{1}_d \otimes \mathcal{O}_A^T)) = \text{tr}_{CA}(\langle \Omega| (\mathbb{1}_d \otimes \mathcal{O}_A^T)(\rho_C \otimes \mathbb{1}_d) |\Omega\rangle_{CA},$$

where ρ_C and \mathcal{O}_A are bounded linear operators in d -dimensional Hilbert space. In the second case, a closed circle formed by two oblique lines for transfer operators

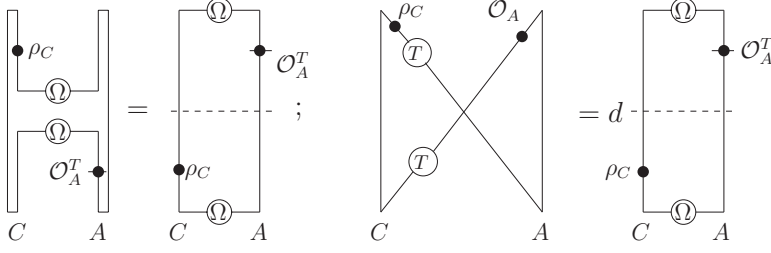


FIGURE 13. Closed circles using cup and cap or oblique lines.

denotes a same trace as a top cap with a bottom cup, which is algebraically proved,

$$\begin{aligned}
 \text{tr}_{CA}((\rho_C T_{CA})(\mathcal{O}_A T_{AC})) &= \sum_{i,j=0}^{d-1} \text{tr}_{CA}((\rho_C |e_i\rangle_{CA} \langle e_i|)(\mathcal{O}_A |e_j\rangle_{AC} \langle e_j|)) \\
 &= \sum_{i,j=0}^{d-1} \text{tr}_{CA}((\rho_C |e_i\rangle_C \otimes \mathcal{O}_A |e_j\rangle_A)(\langle e_j|_A \otimes \langle e_i|_C)) \\
 &= \sum_{i,j=0}^{d-1} (\rho_C)_{ji} (\mathcal{O}_A)_{ij} = \text{tr}(\rho_C \mathcal{O}_A) \\
 (61) \quad &= d \cdot {}_C A \langle \Omega | (\rho_C \otimes \mathbb{1}_d) (\mathbb{1}_d \otimes \mathcal{O}_A^T) | \Omega \rangle_{CA}.
 \end{aligned}$$

Example 5: Figure 14 recognizes the configuration of cup (cap) as compositions of cups and caps. In the left diagrammatical term, the cup $|\Omega\rangle_{AD}$ is a result of connecting the cap ${}_B C \langle \Omega |$ with the cups $|\Omega\rangle_{AB}$ and $|\Omega\rangle_{CD}$, which is verified after some algebra

$$\begin{aligned}
 &({}_B C \langle \Omega |)(|\Omega\rangle_{AB})(|\Omega\rangle_{CD}) \\
 \equiv &(\mathbb{1}_d \otimes {}_B C \langle \Omega | \otimes \mathbb{1}_d)(|\Omega\rangle_{AB} \otimes \mathbb{1}_d \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes \mathbb{1}_d \otimes |\Omega\rangle_{CD}) \\
 = &\frac{1}{d\sqrt{d}} \sum_{i,j,k=0}^{d-1} (\langle e_i^B \otimes e_i^C |)(|e_j^A \otimes e_j^B\rangle)(|e_k^C \otimes e_k^D\rangle) \\
 (62) \quad = &\frac{1}{d\sqrt{d}} \sum_{i=0}^{d-1} |e_i^A \otimes e_i^D\rangle = \frac{1}{d} |\Omega\rangle_{AD}.
 \end{aligned}$$

The right diagrammatical term shows the cap ${}_A D \langle \Omega |$ as a composition of the caps ${}_A B \langle \Omega |$, ${}_C D \langle \Omega |$ and the cup $|\Omega\rangle_{BC}$,

$$\begin{aligned}
 &({}_A B \langle \Omega |)({}_C D \langle \Omega |)(|\Omega\rangle_{BC}) \\
 (63) \equiv &({}_A B \langle \Omega | \otimes \mathbb{1}_d \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes \mathbb{1}_d \otimes {}_C D \langle \Omega |)(\mathbb{1}_d \otimes |\Omega\rangle_{BC} \otimes \mathbb{1}_d) = \frac{1}{d} {}_A D \langle \Omega |.
 \end{aligned}$$

As a remark, the above examples will be exploited in the following sections as topological-like diagrammatical tricks [34] in the extended TL diagrammatical configuration for quantum information and computation.

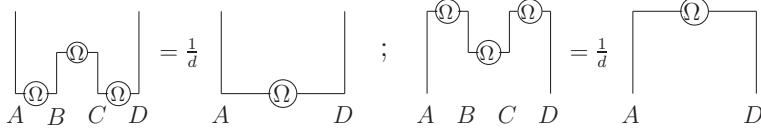


FIGURE 14. Cup and cap as compositions of cups and caps.

4. Extended TL diagrammatical approach (II): quantum teleportation

Three types of descriptions for quantum teleportation: quantum information flow denoted by the transfer operator, measurement-based quantum computation, and tight teleportation scheme, are unified in the extended TL diagrammatical approach.

4.1. Quantum teleportation using the transfer operator. Quantum teleportation can be formulated using the transfer operator T_{BC} (50) which sends the quantum state from Charlie to Bob in the way: $T_{BC}|\psi\rangle_C = |\psi\rangle_B$, besides its standard description [8, 9] using the teleportation equation (8). The entire teleportation process involves local unitary transformations which are not shown in the formalism (51) of the transfer operator T_{BC} . To be general, therefore, we recall the calculation [43] to reformulate the transfer operator in terms of maximally entangled states $|\Phi(U)\rangle_{CA}$ and $|\Phi(V^T)\rangle_{AB}$ labeled by local unitary actions of U and V^T on $|\Omega\rangle$,

$$\begin{aligned}
 {}_{CA}\langle\Phi(U)|\Phi(V^T)\rangle_{AB} &\equiv {}_{CA}\langle\Omega|(U^\dagger \otimes \mathbb{1}_d)(V^T \otimes \mathbb{1}_d)|\Omega\rangle_{AB} \\
 &\equiv {}_{CAB}\langle\Omega \otimes \mathbb{1}_d|(U^\dagger \otimes \mathbb{1}_d \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes V^T \otimes \mathbb{1}_d)|\mathbb{1}_d \otimes \Omega\rangle_{CAB} \\
 &= {}_{CAB}\langle\Omega \otimes \mathbb{1}_d|(\mathbb{1}_d \otimes \mathbb{1}_d \otimes VU^\dagger)|\mathbb{1}_d \otimes \Omega\rangle_{CAB} \\
 &= \frac{1}{d} \sum_{i=0}^{d-1} {}_{CB}\langle e_i \otimes \mathbb{1}_d|(\mathbb{1}_d \otimes VU^\dagger)|\mathbb{1}_d \otimes e_i\rangle_{CB} \\
 &\equiv \frac{1}{d} \sum_{i=0}^{d-1} {}_C\langle e_i|(VU^\dagger)_B|e_i\rangle_B = \frac{1}{d} \sum_{i=0}^{d-1} (VU^\dagger)_B|e_i\rangle_B {}_C\langle e_i| \\
 (64) \quad &= \frac{1}{d} (VU^\dagger)_B T_{BC}
 \end{aligned}$$

which has a special case of $U = V$ given by

$$(65) \quad \frac{1}{d} T_{BC} = {}_{CA}\langle\Phi(U)|\Phi(U^T)\rangle_{AB}.$$

In Figure 15, we repeat the above algebraic calculation at the diagrammatical level. From the left to the right, the inner product ${}_{CA}\langle\Phi(U)|\Phi(V^T)\rangle_{AB}$ has the $\langle\Omega|$, identity $\mathbb{1}_d$, local unitary operators U and V^T , identity $\mathbb{1}_d$ and $|\Omega\rangle$ which are respectively drawn from the top to the bottom. Move local operators U^\dagger and V^T along the line from their positions to the line denoting the system B , and obtain the product $(VU^\dagger)_B$ of local unitary operators acting on the quantum state that Bob has. The transfer operator T_{BC} has a normalization factor $\frac{1}{d}$ contributed by vanishing of a cup and a cap.

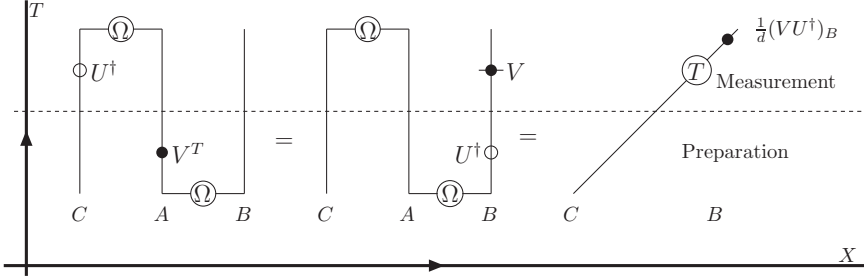


FIGURE 15. Quantum information flow: the transfer operator.

Hence in the extended TL diagrammatical approach, the quantum teleportation can be viewed as a kind of quantum information flow denoted by an oblique line from Charlie to Bob. The result $\frac{1}{d}(VU^\dagger)_B T_{BC}$ seems to argue that quantum measurement labeled by the unitary operator U^\dagger plays a role before state preparation labeled by the unitary operator V^T . But it is not true. Let us read Figure 15 in the way where the T -axis denotes the time-arrow and the X -axis denotes the space-distance. Although the quantum information flow seems to start from the state preparation, pass through the quantum measurement, and come back to the state preparation again, and eventually return to the quantum measurement, it flows from the state preparation to the quantum measurement without violating the causality principle in its final form denoted by an oblique line.

Note that we have to add a rule on how to move operators in the extended TL diagrammatical approach: It is forbidden for an operator to cross over another operator. For example, we have the operator product $\frac{1}{d}(VU^\dagger)_B$ instead of $\frac{1}{d}(U^\dagger V)_B$. Obviously, a violation of this rule leads to a violation of the causality principle. In addition, there are another known approaches to the quantum information flow: the teleportation topology [13, 29] and categorical approach [46], which will be compared with the extended TL diagrammatical approach in Section 7.

4.2. Measurement-based quantum teleportation. Quantum teleportation can be described from the point of quantum measurement [37, 38, 39, 50]. The difference from its standard description [8, 9] is that the maximally entangled state $|\Omega\rangle_{AB}$ between Alice and Bob is created via quantum measurement [37]. Here it is convenient to represent a quantum measurement in terms of a projector $(|\Omega\rangle\langle\Omega|)_{AB}$. Therefore, quantum teleportation is determined by two quantum measurements: the one denoted by $(|\Omega\rangle\langle\Omega|)_{AB}$ and the other denoted by $(|\Omega_n\rangle\langle\Omega_n|)_{CA}$, which leads to a new formulation of the teleportation equation,

$$(66) \quad (|\Omega_n\rangle\langle\Omega_n| \otimes \mathbb{1}_d)(|\psi\rangle \otimes |\Omega\rangle\langle\Omega|) = \frac{1}{d}(|\Omega_n\rangle \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes (\mathbb{1}_d \otimes U_n^\dagger)|\psi\rangle)\langle\Omega|,$$

where lower indices A, B, C are omitted for convenience. Read this teleportation equation (66) from the left to the right, and draw the diagram from the top to the bottom in view of the extended TL diagrammatical rules, i.e., Figure 16.

There is a natural connection between two formalisms (8) and (66) of the teleportation equation. Consider all unitary matrices U_n satisfying (52) and (53), and then make a summation of all teleportation equations of the type (66) labeled

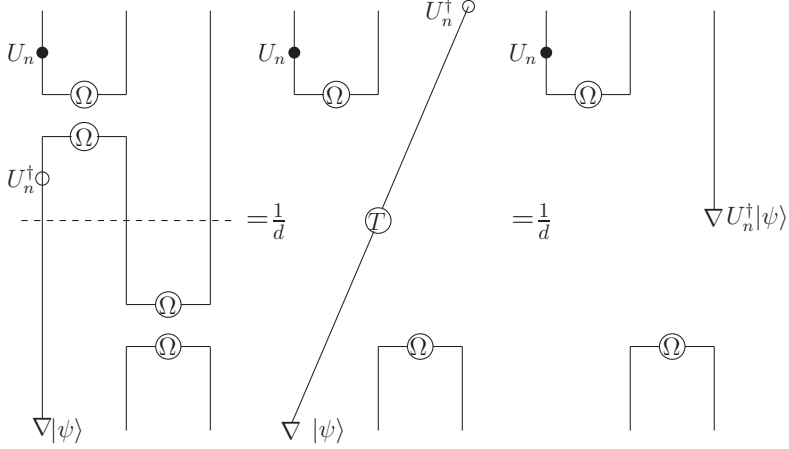


FIGURE 16. Measurement-based quantum teleportation.

by U_n to derive

$$(67) \quad |\psi\rangle \otimes |\Omega\rangle = \frac{1}{d} \sum_{n=1}^{d^2} |\Omega_n\rangle \otimes U_n^\dagger |\psi\rangle$$

which is a generalization of the teleportation equation of the type (8) in the d -dimension Hilbert space. As $d = 2$, the collection of the basis of unitary operators consist of unit matrix $\mathbb{1}_2$ and Pauli matrices $\sigma_1, \sigma_2, \sigma_3$. Bell measurements are denoted by projectors in terms of Bell states $|\phi^\pm\rangle$ and $|\psi^\pm\rangle$. They lead to the same kind of the teleportation equations of the type (66),

$$(68) \quad \begin{aligned} (|\phi^-\rangle\langle\phi^-| \otimes \mathbb{1}_2)(|\psi\rangle \otimes |\phi^+\rangle) &= \frac{1}{2}(|\phi^-\rangle \otimes \sigma_3|\psi\rangle), \\ (|\psi^+\rangle\langle\psi^+| \otimes \mathbb{1}_2)(|\psi\rangle \otimes |\phi^+\rangle) &= \frac{1}{2}(|\psi^+\rangle \otimes \sigma_1|\psi\rangle), \\ (|\psi^-\rangle\langle\psi^-| \otimes \mathbb{1}_2)(|\psi\rangle \otimes |\phi^+\rangle) &= \frac{1}{2}(|\psi^-\rangle \otimes -i\sigma_2|\psi\rangle), \\ (|\phi^+\rangle\langle\phi^+| \otimes \mathbb{1}_2)(|\psi\rangle \otimes |\phi^+\rangle) &= \frac{1}{2}(|\phi^+\rangle \otimes |\psi\rangle), \end{aligned}$$

which has a summation as the teleportation equation (8) since Bell states $|\phi^\pm\rangle$ and $|\psi^\pm\rangle$ satisfy

$$(69) \quad \mathbb{1}_2 = |\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-|.$$

Furthermore, we comment on measurement-based quantum teleportation using continuous variables [38], which is a simple generalization of the discrete teleportation without essential conceptual changes. A maximally entangled state $|\Omega'\rangle$ and teleported state $|\Psi\rangle$ in the continuous case have the form,

$$(70) \quad |\Omega'\rangle = \int dx |x, x\rangle, \quad |\Psi\rangle = \int dx \psi(x) |x\rangle,$$

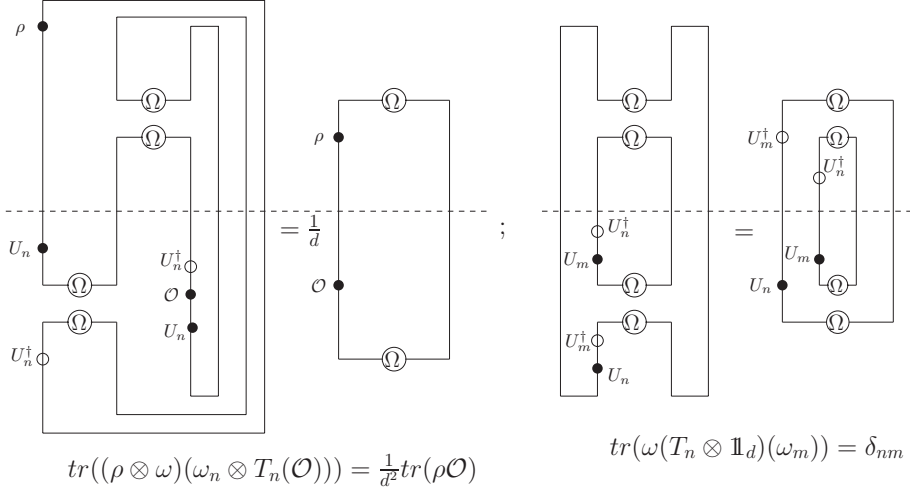


FIGURE 17. Characteristic equations for tight teleportation and dense coding.

and other maximally entangled states $|\Omega'_{\alpha\beta}\rangle$ are formulated by the combined action of the $U(1)$ rotation with the translation T on $|\Omega'\rangle$,

$$(71) \quad |\Omega'_{\alpha\beta}\rangle = (U_\beta \otimes T_\alpha)|\Omega'\rangle \equiv \int dx \exp(i\beta x)|x, x + \alpha\rangle, \quad \alpha, \beta \in \mathbb{R}$$

where $U_\beta|x\rangle = e^{i\beta x}|x\rangle$, $T_\alpha|x\rangle = |x + \alpha\rangle$ and which is a common eigenvector of the location operator $\mathbf{X} \otimes \mathbb{1} - \mathbb{1} \otimes \mathbf{X}$ and conjugate momentum operator $\mathbf{P} \otimes \mathbb{1} + \mathbb{1} \otimes \mathbf{P}$,

$$(72) \quad (\mathbf{X} \otimes \mathbb{1} - \mathbb{1} \otimes \mathbf{X})|\Omega'_{\alpha\beta}\rangle = -\alpha|\Omega'_{\alpha\beta}\rangle, \quad (\mathbf{P} \otimes \mathbb{1} + \mathbb{1} \otimes \mathbf{P})|\Omega'_{\alpha\beta}\rangle = 2\beta|\Omega'_{\alpha\beta}\rangle.$$

The teleportation equation of the type (66) is obtained to be

$$(73) \quad (|\Omega'_{\alpha\beta}\rangle\langle\Omega'_{\alpha\beta}| \otimes \mathbb{1})(|\Psi\rangle \otimes |\Omega'\rangle) = (|\Omega'_{\alpha\beta}\rangle \otimes \mathbb{1})(\mathbb{1} \otimes \mathbb{1} \otimes U_{-\beta}T_\alpha|\Psi\rangle)$$

which has a similar diagrammatical representation as Figure 16. The translation operator T_α is its own adjoint operator, and hence it is permitted to move along a cup or cap without change.

As a remark, the difference between Figure 15 and 16 lies in there are an extra cup and cap besides the quantum information flow in Figure 15, which become crucial when we study the tight teleportation scheme in the next subsection. In addition, Figure 16 is a typical configuration in the diagrammatical representation for the TL algebra as involved local unitary operators are identity, see Section 5.

4.3. Tight teleportation and dense coding schemes. In the tight teleportation and dense coding schemes [30], all involved finite Hilbert spaces are d dimensional and the classical channel distinguishes d^2 signals. All examples we treated in the above belong to the tight class. We exploit the same notations as in [30]. The density operator ρ is a positive operator with a normalized trace. Charlie has his density operator $\rho_C = (|\phi_1\rangle\langle\phi_2|)_C$ which denotes the quantum state to be sent to Bob. Alice and Bob share the maximally entangled state ω_{AB} . The set of observables ω_n , $n = 1, 2, \dots, d^2$ over an output parameter space is a collection of bounded linear operators in the Hilbert space \mathcal{H} . Alice performs Bell measurements

in the composite system between Charlie and her, and she chooses her observables $(\omega_n)_{CA}$ as local unitary transformations of the maximally entangled state ω . After Bob gets the message denoted by n from Alice, he applies a local unitary transformation T_n on his observable \mathcal{O}_B , given by

$$(74) \quad T_n(\mathcal{O}_B) = U_n^\dagger \mathcal{O}_B U_n, \quad \mathcal{O}_B = (|\psi_1\rangle\langle\psi_2|)_B, \quad n = 1, 2, \dots, d^2.$$

The operator T_n defined this way is called a channel, a complete positive linear operator with the normalization $T_n(\mathbb{1}_d) = \mathbb{1}_d$.

In terms of ρ_C , ω_{AB} , $(\omega_n)_{CA}$ and $T_n(\mathcal{O}_B)$, the tight teleportation scheme is summarized in the equation

$$(75) \quad \sum_{n=1}^{d^2} \text{tr}((\rho \otimes \omega)(\omega_n \otimes T_n(\mathcal{O}))) = \text{tr}(\rho \mathcal{O}),$$

where lower indices A, B, C are neglected and which is called the characteristic equation for quantum teleportation in our previous work [34]. It catches the aim of a successful teleportation: Charlie performs quantum measurement in his system as he does in Bob's system, though they are far away from each other. The term containing the message n has a form denoted by term_n in the following

$$(76) \quad \begin{aligned} \text{term}_n &= \text{tr}((|\phi_1\rangle\langle\phi_2| \otimes |\Omega\rangle\langle\Omega|)(|\Omega_n\rangle\langle\Omega_n| \otimes U_n^\dagger |\psi_1\rangle\langle\psi_2| U_n)) \\ &= \langle\Omega_n \otimes \psi_2 U_n | \phi_1 \otimes \Omega\rangle \langle\phi_2 \otimes \Omega | \Omega_n \otimes U_n^\dagger \psi_1\rangle \\ &= \left(\frac{1}{d} \langle\psi_2 | \phi_1\rangle\right) \left(\frac{1}{d} \langle\phi_2 | \psi_1\rangle\right) = \frac{1}{d^2} \text{tr}(\rho \mathcal{O}), \end{aligned}$$

where the inner product (54) is applied twice. There are d^2 distinguished messages labeled by n , so we prove the characteristic equation (75). In the left term of Figure 17, we have two ways of deriving the characteristic equation (75) at the diagrammatical level. The first moves local operators U_n^\dagger , \mathcal{O} and U_n from the branch of the cap to the other branch and then applies known diagrammatical tricks by the first term of Figure 12 and the first term of Figure 13. The second makes use of tricks by the second and third terms of Figure 12 and the second term of Figure 13. In addition, the number of classical channel, d^2 counts all possible teleportation diagrams of the same type.

In view of tight dense coding schemes have the same elements as the tight teleportation, all the tight dense coding schemes [30] are concluded in the characteristic equation,

$$(77) \quad \text{tr}(\omega(T_n \otimes \mathbb{1}_d)(\omega_m)) = \delta_{nm}$$

which is explained as follows. As Alice and Bob share the maximally entangled state $|\Omega\rangle_{AB}$, she transforms her state by the channel T_n to encode the message n , and then Bob performs the measurement on observables ω_m in his system. At $n = m$, Bob gets the message. The entire process of dense coding is performed in the way

$$(78) \quad \begin{aligned} &\text{tr}(|\Omega\rangle\langle\Omega|(U_n^\dagger \otimes \mathbb{1}_d)|\Omega_m\rangle\langle\Omega_m|(U_n \otimes \mathbb{1}_d)) \\ &= \langle\Omega|U_n^\dagger \otimes \mathbb{1}_d|\Omega_m\rangle\langle\Omega_m|U_n \otimes \mathbb{1}_d|\Omega\rangle = \frac{1}{d^2} (\text{tr}(U_n^\dagger U_m))^2 = \delta_{nm} \end{aligned}$$

which derives the characteristic equation for tight dense coding (77), also proved in the right term of Figure 17.

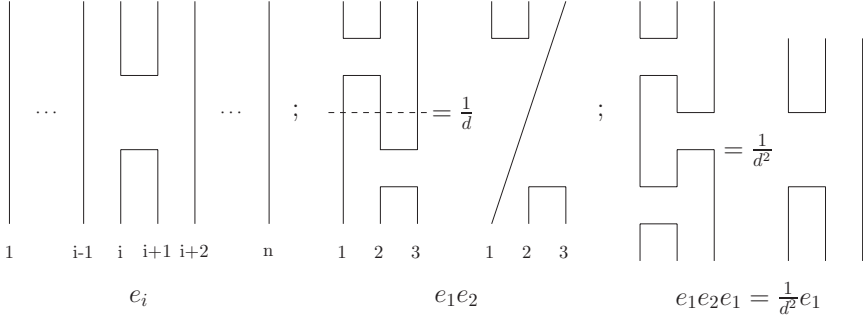


FIGURE 18. Generator e_i , multiplication $e_1 e_2$ and the axiom for the $TL_3(d)$ algebra.

As a remark, Figure 16 denoting measurement-based quantum computation includes all elements of quantum teleportation: Figure 15 representing the quantum information flow is its part, and the left term of Figure 17 is its closure. Therefore, three approaches to quantum teleportation are unified in the extended TL diagrammatical approach.

5. Extended TL diagrammatical approach (III): TL algebra and Brauer algebra

We study algebraic structures in the extended TL diagrammatical approach: the TL algebra, the Brauer algebra, and the extended TL category. Note that symbols Ω labeling maximally entangled states are omitted for convenience without confusion in Figures 18, 19, 21.

5.1. Diagrammatical representation of TL algebra. The TL algebra $TL_n(\lambda)$ over the complex field \mathbb{C} is generated by identity Id and $n - 1$ Hermitian projectors e_i satisfying

$$(79) \quad \begin{aligned} e_i^2 &= e_i, & (e_i)^\dagger &= e_i, \quad i = 1, \dots, n-1, \\ e_i e_{i\pm 1} e_i &= \lambda^{-2} e_i, & e_i e_j &= e_j e_i, \quad |i - j| > 1, \end{aligned}$$

with λ called loop parameter¹. The diagrammatical representation of the TL algebra is called the Brauer diagram [41] or Kauffman diagram [10] in literature. It is a planar (n, n) diagram including a “hidden” rectangle in the plane with $2n$ “hidden” distinct points: n points on its top edge and n points on its bottom edge, and they are connected by disjoint strings drawn in the rectangle. The identity is a diagram with all strings vertical, and e_i has its i th and $i + 1$ th top (bottom) boundary points connected with all other strings vertical. The multiplication $e_i e_j$ identifies bottom points of e_i with corresponding top points of e_j , removes a common boundary, and replaces each obtained loop with a factor λ . The adjoint of e_i is its image under a mirror reflection on a horizontal line.

¹The notation e_i for an idempotent of the TL algebra is easily confused with a basis vector $|e_i\rangle$. As they both appear in the same subsection, we denote $|e_i\rangle$ by $|i\rangle$.

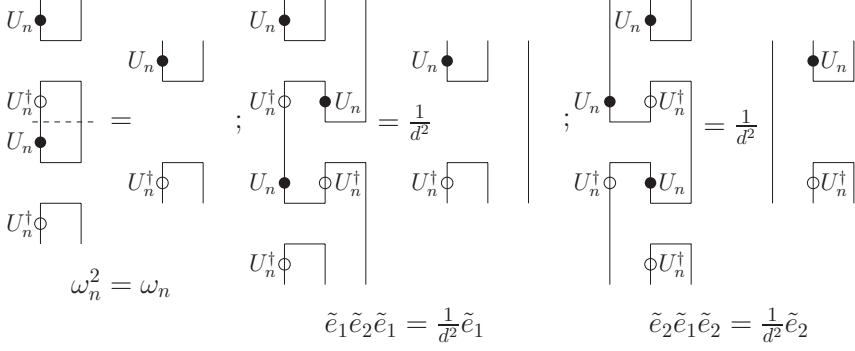


FIGURE 19. The $TL_3(d)$ algebra in the extended TL diagrammatic approach.

Let us set up a representation of the $TL_n(d)$ algebra in terms of the maximally entangled state ω ,

$$(80) \quad \omega = |\Omega\rangle\langle\Omega| = \frac{1}{d} \sum_{i,j=0}^{d-1} |ii\rangle\langle jj|, \quad \omega^2 = \omega$$

by defining idempotents e_i as

$$(81) \quad e_i = (Id)^{\otimes(i-1)} \otimes \omega \otimes (Id)^{\otimes(n-i-1)}, \quad i = 1, \dots, n-1$$

with loop parameter d . For example, a representation of the $TL_3(d)$ algebra is generated by two idempotents e_1 and e_2 ,

$$(82) \quad e_1 = \omega \otimes Id, \quad e_2 = Id \otimes \omega,$$

and they proved to satisfy the axiom $e_1 e_2 e_1 = \frac{1}{d^2} e_1$ in the way

$$(83) \quad e_1 e_2 e_1 |\alpha\beta\gamma\rangle = \frac{1}{d} \sum_{l=0}^{d-1} e_1 e_2 |ll\gamma\rangle \delta_{\alpha\beta} = \frac{1}{d^3} \sum_{n=0}^{d-1} |nn\gamma\rangle \delta_{\alpha\beta} = \frac{1}{d^2} e_1 |\alpha\beta\gamma\rangle$$

as well as the axiom $e_2 e_1 e_2 = \frac{1}{d^2} e_2$ using similar calculation. Figure 18 is a diagrammatical representation for e_i , $e_1 e_2$ and $e_1 e_2 e_1 = \frac{1}{d^2} e_1$ with loop parameter d . Therefore, a cup (cap) introduced in the extended TL diagrammatical approach is a connected line between top (bottom) boundary points. Each cup (cap) with a normalization factor $d^{-\frac{1}{2}}$ leads to an additional normalization factor $d^{-\frac{1}{2}N}$ as the number of vanishing cups and caps is N , and a closed circle yields a normalization factor $d = \text{tr}(\mathbb{1}_d)$. For examples, $e_1 e_2$ has a normalization factor $\frac{1}{d}$ from a vanishing cup and cap, and $e_1 e_2 e_1$ has a factor $\frac{1}{d^2}$ from four vanishing cups and caps.

In terms of the maximally entangled state ω_n as a local unitary transformation U_n of ω , we can set up a representation of the $TL_n(d)$ algebra, too. For example, a representation of the $TL_3(d)$ algebra is generated by \tilde{e}_1 and \tilde{e}_2 ,

$$(84) \quad \tilde{e}_1 = \omega_n \otimes Id, \quad \tilde{e}_2 = Id \otimes \omega_n,$$

which are proved to satisfy the axioms of the TL algebra in the extended TL diagrammatical approach, see Figure 19. Hence the axioms of the TL algebra are

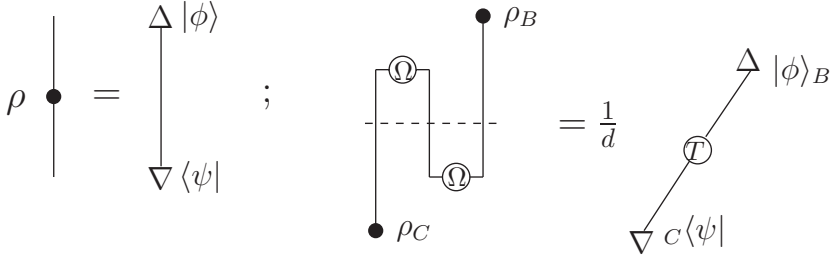


FIGURE 20. Quantum information flow with the density operator.

invariant under local unitary transformations as idempotents e_i are generated by the maximally entangled state ω .

Furthermore, a representation of the $TL_3(d)$ algebra is constructed in the way

$$(85) \quad e'_1 = \rho \otimes \omega, \quad e'_2 = \omega \otimes \rho, \quad \rho = |\phi\rangle\langle\psi|, \quad \text{tr}(\rho) = 1.$$

because ρ and ω and the tensor products between them are all projectors. The axioms of the TL algebra are checked in both algebraic and diagrammatical approaches. Do calculation

$$(86) \quad \begin{aligned} (\omega \otimes \rho)(\rho \otimes \omega) &= \frac{1}{d^2} \sum_{i,j=0}^{d-1} (|ii\rangle\langle jj| \otimes |\phi\rangle\langle\psi|) \sum_{l,m=0}^{d-1} (|\phi\rangle\langle\psi| \otimes |ll\rangle\langle mm|) \\ &= \frac{1}{d^2} \sum_{i,j=0}^{d-1} \sum_{l,m=0}^{d-1} (|ii\phi\rangle\langle jj\psi|)(|\phi ll\rangle\langle\psi mm|) = \frac{1}{d^2} \sum_{i,j=0}^{d-1} |ii\phi\rangle\langle\psi jj| \end{aligned}$$

which leads to a proof for the axiom $e'_2 e'_1 e'_2 = \frac{1}{d^2} e'_2$,

$$(87) \quad \begin{aligned} (\omega \otimes \rho)(\rho \otimes \omega)(\omega \otimes \rho) &= \frac{1}{d^3} \sum_{i,j=0}^{d-1} \sum_{l,m=0}^{d-1} |ii\phi\rangle\langle\psi jj| |ll\phi\rangle\langle mm\psi| \\ &= \frac{1}{d^2} \sum_{i,j=0}^{d-1} |ii\phi\rangle\langle jj\psi| = \frac{1}{d^2} (\omega \otimes \rho). \end{aligned}$$

Similarly to prove $e'_1 e'_2 e'_1 = \frac{1}{d^2} e'_1$. As a remark, $\rho = |\phi\rangle\langle\psi|$ so that the transfer operator T_{BC} sends a half of ρ_C , $|\phi\rangle_C$ from Charlie to Bob to form a unit inner product with ${}_B\langle\psi|$, a half of ρ_B , see Figure 20. Moreover, in terms of ρ and ω_n , a representation of the $TL_3(d)$ algebra is also set up in another way

$$(88) \quad \tilde{e}'_1 = \rho \otimes \omega_n, \quad \tilde{e}'_2 = \omega_n \otimes \rho, \quad n = 1, \dots, d^2,$$

if and only if a local unitary transformation U_n is a symmetric matrix:

$$(89) \quad U_n^T = U_n, \quad U_n^T U_n^\dagger = U_n^* U_n = \mathbb{1}_d$$

which can be observed in Figure 19.

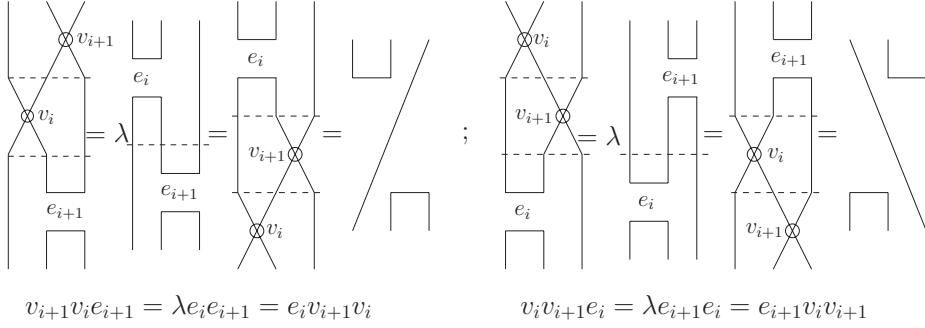


FIGURE 21. Quantum teleportation: the Brauer algebra.

5.2. Quantum Teleportation: the Brauer algebra. Quantum teleportation has a same diagrammatical representation as the element $e_1 e_2$ ($e_2 e_1$) of the TL algebra, if involved local unitary transformations are identity (see Figure 16). There exists a natural question which can be possibly asked. Quantum teleportation plays important roles in quantum information, but the product $e_1 e_2$ ($e_2 e_1$) is only an element of the TL algebra. It is meaningful to explore in which case the configuration of $e_1 e_2$ ($e_2 e_1$) is crucial in the mathematical sense. In the following, we present the axioms of the Brauer algebra [41] and explain that the quantum teleportation configuration forms a bone of this algebra.

The Brauer algebra $D_n(\lambda)$ is an extension of the TL algebra with virtual crossings, λ called loop parameter. It has two types of generators: idempotents e_i of the TL algebra $TL_n(\lambda)$ satisfying (79) and virtual crossings v_i satisfying (26), $i = 1, \dots, n-1$. Both generators satisfy the mixed relations of the Brauer algebra,

$$(90) \quad \begin{aligned} (ev/v_e) : & \quad e_i v_i = v_i e_i = e_i, \quad e_i v_j = v_j e_i, \quad j \neq i \pm 1, \\ (vve) : & \quad v_{i\pm 1} v_i e_{i\pm 1} = \lambda e_i e_{i\pm 1}, \quad (evv) : \quad e_i v_{i\pm 1} v_i = \lambda e_i e_{i\pm 1} \end{aligned}$$

which has a diagrammatical representation in Figure 21. For example, the permutation P as a virtual crossing and the maximally entangled state ω as an idempotent

$$(91) \quad P = \sum_{i,j=0}^{d-1} |i \otimes j\rangle \langle j \otimes i|, \quad \omega = \frac{1}{d} \sum_{i=0}^{d-1} |i \otimes i\rangle \langle j \otimes j|$$

form a representation of the Brauer algebra $D_2(d)$ with loop parameter d . The axiom (ev/v_e) is verified in the way

$$(92) \quad P\omega = \frac{1}{d} \sum_{i,j=0}^{d-1} \sum_{i',j'=0}^{d-1} |i \otimes j\rangle \langle j \otimes i| |i' \otimes i'\rangle \langle j' \otimes j'| = \omega = \omega P,$$

and the axioms (vve) and (eev) are proved after some algebra

$$\begin{aligned} (\mathbb{1}_d \otimes P)(P \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes \omega) &= d(\omega \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes \omega) = (\omega \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes P)(P \otimes \mathbb{1}_d), \\ (P \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes P)(\omega \otimes \mathbb{1}_d) &= d(\mathbb{1}_d \otimes \omega)(\omega \otimes \mathbb{1}_d) = (\mathbb{1}_d \otimes \omega)(P \otimes \mathbb{1}_d)(\mathbb{1}_d \otimes P), \end{aligned}$$

which are also proved in Figure 21 with $\lambda = d$.

As a remark on Figure 21, it is clear that the configuration for quantum teleportation is fundamental for defining the Brauer algebra. The Brauer algebra presents an equivalent approach of performing the teleportation using the swap

gate P and Bell measurement, where the teleportation swapping $(P \otimes Id)(Id \otimes P)$ or $(Id \otimes P)(P \otimes Id)$ are involved. As a summary of algebraic structures underlying quantum teleportation, we have proposed the braid teleportation, the teleportation swapping, the virtual braid teleportation, the Temperley–Lieb algebra, and the Brauer algebra.

5.3. Comment on the extended TL category. In this paper, we propose the extended TL diagrammatical approach to quantum information and computation involving maximally entangled states and local unitary transformations. Its diagrammatical configurations consist of cups, caps, solid points, empty circles, etc., as an extension of Kauffman diagrams or Brauer diagrams. An extension of the TL algebra with local unitary transformations is called *the extended TL algebra*, and the collection of all extended TL algebras is called *the extended TL category* which contains abundant mathematical objects such as braids, permutation, the TL algebra, the Brauer algebra, and others (see the next section). This category is a mathematical foundation of our diagrammatical approach.

Furthermore, interested readers are invited to refer our previous work [34], in which *unitary Hermitian ribbon categories* are suggested as a mathematical description of quantum information and physics as well as the extended TL diagrammatical approach is viewed as a diagrammatical representation for tensor categories.

6. Extended TL diagrammatical approach (IV): entanglement swapping and universal quantum computation

We study the entanglement swapping, universal quantum computing, and multipartite entanglements, in the extended TL diagrammatical approach which is a diagrammatical representation for the extended TL category.

6.1. Entanglement swapping. Entanglement swapping [44] is an experimental technique realizing quantum entanglement between two independent systems as a consequence of quantum measurement instead of physical interaction. Let us make an example for its theoretical interpretation in terms of a projector representing quantum measurement. Alice has a bipartite entangled state $|\Omega_l\rangle_{ab}^A$ for particles a, b , and Bob has $|\Omega_m\rangle_{cd}^B$ for particles c, d . They are independently created and do not share common history. Alice applies quantum measurement denoted by $Id \otimes |\Omega_n\rangle\langle\Omega_n| \otimes Id$ to the product state of $|\Omega_l\rangle_{ab}^A$ and $|\Omega_m\rangle_{cd}^B$, so that the output called the entanglement swapped state $|\Omega_{lnm}\rangle_{ad}^{AB}$ is a bipartite entangled state shared by Alice and Bob for particles a, d ,

$$\begin{aligned}
 & (Id \otimes |\Omega_n\rangle\langle\Omega_n| \otimes Id)(|\Omega_l\rangle_{ab}^A \otimes |\Omega_m\rangle_{cd}^B) \\
 &= \frac{1}{d}(Id \otimes |\Omega_n\rangle \otimes Id) \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} (U_l U_n^* U_m |e_i\rangle_a^A \otimes Id \otimes Id \otimes |e_i\rangle_d^B) \\
 (93) \quad & \equiv \frac{1}{d}(Id \otimes |\Omega_n\rangle \otimes Id) |\Omega_{lnm}\rangle_{ad}^{AB}.
 \end{aligned}$$

In other words, the entanglement swapping reduces a four-particle state $|\Omega_l\rangle_{ab}^A \otimes |\Omega_m\rangle_{cd}^B$ to a bipartite entangled state $|\Omega_{lnm}\rangle_{ad}^{AB}$ using entangling measurement. As a remark, the entanglement swapped state $|\Omega_{lnm}\rangle_{ad}^{AB}$ plays a role in the comparison of quantum mechanics with classical physics, because it is a quantum state but produced without any classical physical interactions.

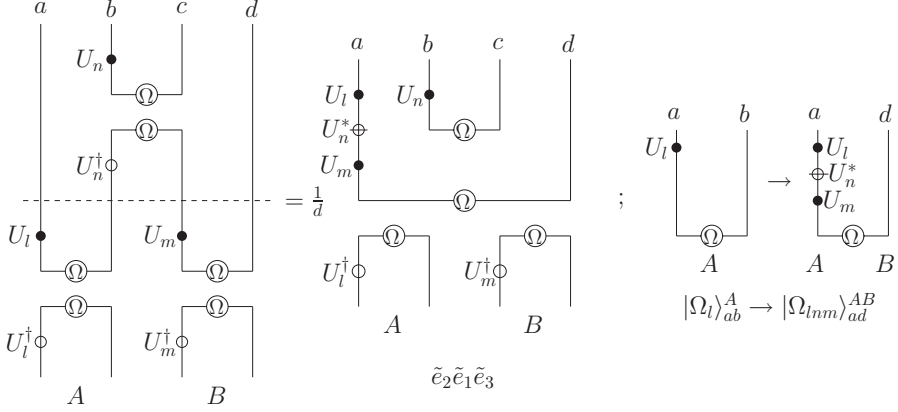


FIGURE 22. Entanglement swapping in the extended TL category.

Read the entanglement swapping equation (93) from the left to the right and draw a diagram from the top to the bottom according to the extended TL diagrammatical rules, i.e., the left term of Figure 22. It is a configuration for an element $\tilde{e}_2 \tilde{e}_1 \tilde{e}_3$ in the extended TL category, i.e.,

$$(94) \quad \tilde{e}_2 \tilde{e}_1 \tilde{e}_3 = (Id \otimes \omega_n \otimes Id)(\omega_l \otimes Id \otimes Id)(Id \otimes Id \otimes \omega_m).$$

which changes the entangled state $|\Omega_l\rangle_{ab}^A$ in Alice's system to the entangled state $|\Omega_{lnm}\rangle_{ad}^{AB}$ in Alice and Bob's composite system, see the right term of Figure 22. Furthermore, the entanglement swapping is also called the teleportation using a cup state. Alice measures the Bell state $|\Omega\rangle_{AB}$ with a projector $|\psi\rangle_A \langle \psi|$ so that she transfers her quantum state $|\psi\rangle_A$ to Bob in the way

$$(95) \quad \begin{aligned} |\psi\rangle_A \langle \psi| \Omega_{AB} &= \frac{1}{\sqrt{d}} |\psi\rangle_A \sum_{i,j=0}^{d-1} {}_{AB} \langle e_j \otimes Id | \psi_j^* | e_i \otimes e_i \rangle_{AB} \\ &= \frac{1}{\sqrt{d}} |\psi\rangle_A \sum_{i=0}^{d-1} \psi_i^* | e_i \rangle_B = \frac{1}{\sqrt{d}} |\psi\rangle_A (\langle \psi |)_B^T, \end{aligned}$$

which has a diagrammatical representation, the left term of Figure 23 with $(\langle e_i |)^T = |e_i\rangle$, similar to the two-way teleportation in the crossed measurement [38, 50].

The characteristic equation for the tight entanglement swapping is derived by a similar procedure of obtaining characteristic equations for tight teleportation and dense coding schemes [30],

$$(96) \quad \sum_{n=1}^{d^2} \text{tr}((\rho \otimes \omega_n \otimes T_n(\mathcal{O}))(\omega \otimes \omega)) = \frac{1}{d} \text{tr}(\rho \mathcal{O}^T)$$

where the density operator ρ for particle a , observable \mathcal{O} for particle d , and quantum channel $T_n(\mathcal{O})$ for particle d are respectively given by

$$(97) \quad \rho = |\phi_1\rangle \langle \phi_2|, \quad \mathcal{O} = |\psi_1\rangle \langle \psi_2|, \quad T_n(\mathcal{O}) = U_n^\dagger \mathcal{O} U_n$$

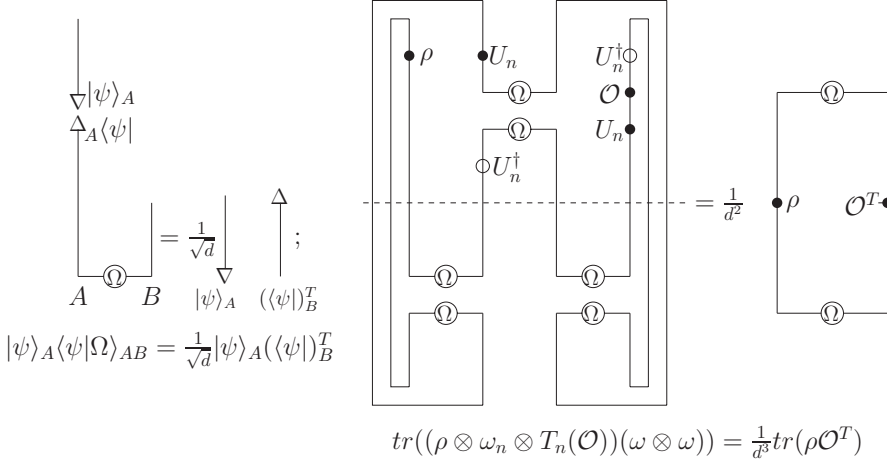


FIGURE 23. Tight entanglement swapping in the extended TL category.

and the transpose of the density operator, \mathcal{O}^T is defined in the way

$$(98) \quad \mathcal{O}^T = \sum_{i,j=0}^{d-1} \psi_{1i} \psi_{2j}^* (|e_i\rangle \langle e_j|)^T = \sum_{i,j=0}^{d-1} \psi_{1i} \psi_{2j}^* |e_j\rangle \langle e_i|, \quad (\langle e_i|)^T = |e_i\rangle.$$

The tight entanglement swapping equation (96) is easily proved in the extended TL diagrammatical approach, see the right term of Figure 23 which is a closure of the left term of Figure 22. The diagrammatical trick by Figure 14 is exploited to derive the same configuration as the first term of Figure 13. It can be also verified in an algebraic way: the $term_n$ given by

$$\begin{aligned}
 term_n &\equiv tr((|\phi_1\rangle \langle \phi_2| \otimes |\Omega_n\rangle \langle \Omega_n| \otimes U_n^\dagger |\psi_1\rangle \langle \psi_2| U_n) (|\Omega\rangle \langle \Omega| \otimes |\Omega\rangle \langle \Omega|)) \\
 &= \langle \phi_2 \otimes \Omega_n \otimes \psi_2 U_n | \Omega \otimes \Omega \rangle \langle \Omega \otimes \Omega | \phi_1 \otimes \Omega_n \otimes U_n^\dagger \psi_1 \rangle \\
 (99) \quad &= \frac{1}{d^3} (\phi_2^* \cdot \psi_2^*) (\phi_1 \cdot \psi_1)
 \end{aligned}$$

is found to be

$$(100) \quad \frac{1}{d^3} tr(\rho \mathcal{O}^T) = \frac{1}{d^3} \sum_{i,j=0}^{d-1} \psi_{1i} \psi_{2j}^* \langle e_i | \phi_1 \rangle \langle \phi_2 | e_j \rangle = term_n,$$

and the characteristic equation (96) is proved due to there are d^2 $term_n$ with each $term_n$ independent of n .

Therefore, the extended TL diagrammatical approach is not only to describe a quantum information protocol but also to assign it a characteristic equation.

6.2. Universal quantum computing. Quantum teleportation has been considered as a universal quantum computational primitive [45]. Under such a proposal, there are both theoretical observations and experimental motivations. The teleported state permits the action of local unitary transformations, and so quantum teleportation realizes single-qubit gates as local unitary transformations and two-qubit gates as linear combinations of products of single-qubit gates. Besides

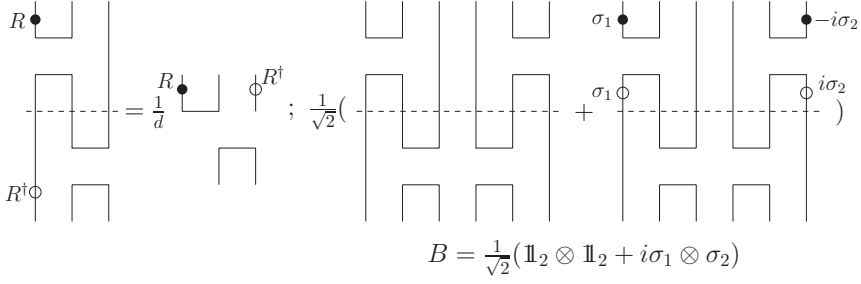


FIGURE 24. Single-qubit gate and unitary braid gate.

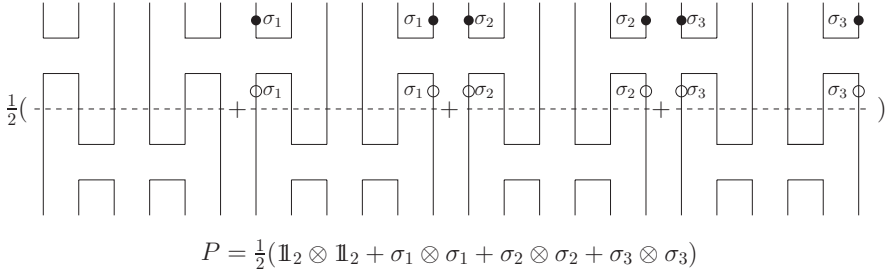


FIGURE 25. Swap gate in the extended TL category

single-qubit transformations and Bell measurements can be performed in labs. Additionally, we have fault-tolerant quantum computation [51, 52], as single-qubit transformations are performed fault-tolerantly.

A fault-tolerant gate R , an element of the Clifford group [51, 52], enters the teleportation via entangling measurement and then is transported in the form of its conjugation R^\dagger , see the left term of Figure 24. A unitary braid gate (9) has a form given by

$$(101) \quad B = \frac{1}{\sqrt{2}}(\mathbb{I}_2 \otimes \mathbb{I}_2 + i\sigma_1 \otimes \sigma_2)$$

which is performed in the way shown in the extended TL diagrammatical approach, see the right term of Figure 24. It has two diagrammatical terms and each one consists of two teleportation processes for sending a two-qubit. The swap gate P , denoted by (34), is an element of the extended TL category, i.e., Figure 25 which has four diagrammatical terms and each one represents an algebraic term in (34). The CNOT gate, a linear combination of products of Pauli matrices,

$$(102) \quad \begin{aligned} CNOT &= (|0\rangle\langle 0| \otimes \mathbb{I}_2 + |1\rangle\langle 1| \otimes \sigma_1) = \frac{1}{2}(\mathbb{I}_2 + \sigma_3) \otimes \mathbb{I}_2 + \frac{1}{2}(\mathbb{I}_2 - \sigma_3) \otimes \sigma_1, \\ &= \frac{1}{2}(\mathbb{I}_2 \otimes \mathbb{I}_2 + \mathbb{I}_2 \otimes \sigma_1 + \sigma_3 \otimes \mathbb{I}_2 - \sigma_3 \otimes \sigma_1) \end{aligned}$$

satisfying basic properties of the CNOT gate,

$$CNOT|00\rangle = |00\rangle, \quad CNOT|01\rangle = |01\rangle, \quad CNOT|10\rangle = |11\rangle, \quad CNOT|11\rangle = |10\rangle,$$

$$CNOT = \frac{1}{2}(\mathbb{1}_2 \otimes \mathbb{1}_2 + \mathbb{1}_2 \otimes \sigma_1 + \sigma_3 \otimes \mathbb{1}_2 - \sigma_3 \otimes \sigma_1)$$

FIGURE 26. CNOT gate in the extended TL category.

is an element of the extended TL category, Figure 26. Note that symbols Ω labeling a cup and cap are omitted in Figures 24-26 for convenience.

Knot polynomial in terms of a unitary braid gate [13, 17, 18] in the extended TL category can be computed using quantum simulation of knot on quantum computer, which is different from an approximate quantum algorithm [53] for computing the Jones polynomial as well as topological quantum computing [54, 55] involving unitary braid representations as quantum gates acting on quasi-particles like anyons. Furthermore, virtual knots can be simulated via a quantum program with unitary braid gates and swap gates. Moreover, exactly solvable two dimensional quantum field theories or statistical models [15, 16] can be simulated on quantum computer, since unitary solutions of the Yang–Baxter equation with spectral parameters [17, 18] can be performed in the extended TL category.

As a remark, the extended TL category is a low-dimensional “topological” model for universal quantum computation, and “topological” or topological-like features [34] are expected to be helpful to look for new quantum algorithms.

6.3. Comment on multipartite entanglements. Bell measurements and local unitary transformations are crucial elements for the application of the extended TL diagrammatical rules. Hence, multipartite maximally entangled states like the GHZ state or the state $|\chi\rangle$ can be treated in the extended TL category if they have a form in terms of Bell measurements and local unitary transformations. For example, the GHZ state $|GHZ\rangle$ is a linear combination of local unitary transformations of Bell state,

$$\begin{aligned}
 |GHZ\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |00\rangle + |1\rangle \otimes |11\rangle) \\
 &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes |\phi^+\rangle + \frac{1}{2}(|0\rangle - |1\rangle) \otimes |\phi^-\rangle \\
 (103) \quad &= \frac{1}{2}(\mathbb{1}_8 + \sigma_3 \otimes \mathbb{1}_2 \otimes \sigma_3)(|\alpha\rangle \otimes |\phi^+\rangle)
 \end{aligned}$$

where $|\alpha\rangle = |0\rangle + |1\rangle$. Similarly, the four-particle state $|\chi\rangle$ [45], in the construction of the CNOT gate using quantum teleportation, has a form

$$\begin{aligned}
 |\chi\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|00\rangle + \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)|11\rangle \\
 &= \frac{1}{\sqrt{2}}|\phi^+\rangle(|\phi^+\rangle + |\phi^-\rangle) + \frac{1}{\sqrt{2}}|\psi^+\rangle(|\phi^+\rangle - |\phi^-\rangle) \\
 (104) \quad &= \frac{1}{\sqrt{2}}(\mathbb{1}_{16} + \mathbb{1}_8 \otimes \sigma_3 + \mathbb{1}_2 \otimes \sigma_1 \otimes \mathbb{1}_4 - \mathbb{1}_2 \otimes \sigma_1 \otimes \mathbb{1}_2 \otimes \sigma_3)|\phi^+\rangle|\phi^+\rangle.
 \end{aligned}$$

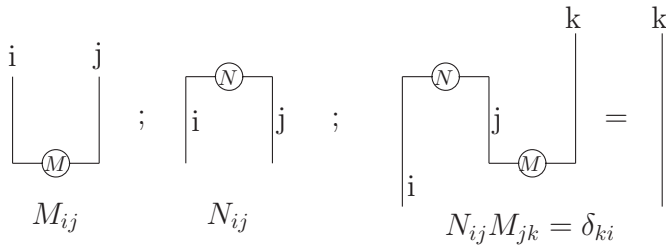


FIGURE 27. Teleportation topology: the topological condition.

We will explore quantum teleportation using multipartite maximally entangled states in the extended TL category in our further research. As a remark, the extended TL diagrammatical approach rules can be applied to topics like Bell inequalities, quantum cryptography and so on, in which Bell measurements and local unitary transformations play fundamental roles.

7. Extended TL diagrammatical approach (V): quantum information flow

We describe the quantum information flow in the extended TL category, and compare this description with another two known approaches: the teleportation topology [13, 29] and strongly compact closed categories [46].

7.1. Teleportation topology. Teleportation topology [13, 29] explains quantum teleportation as a kind of topological amplitude satisfying the topological condition. There are one-to-one correspondences between quantum amplitude and topological amplitude. The state preparation describes a creation of a two-particle quantum state from vacuum with a diagrammatical representation denoted by a cup state $|Cup\rangle$, and quantum measurement denotes an annihilation of a two-particle quantum state with a diagrammatical representation by a cap state $\langle Cap|$. See Figure 27. The cup and cap states are associated with the matrices M and N in the way

$$(105) \quad |Cup\rangle = \sum_{i,j=0}^{d-1} M_{ij} |e_i \otimes e_j\rangle, \quad \langle Cap| = \sum_{i,j=0}^{d-1} \langle e_i \otimes e_j | N_{ij}$$

which satisfy the topological condition, i.e., the concatenation of a cup and a cap is a straight line denoted by the identity matrix $N_{ij}M_{jk} = \delta_{ik}$.

In the extended TL diagrammatical approach, the concatenation of a cup and a cap is formulated by the transfer operator which is not identity required by the topological condition, see Figure 15. Besides, the cup and cap states are normalized maximally entangled states given by

$$(106) \quad |Cup\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i \otimes e_i\rangle, \quad \langle Cap| = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} \langle e_i \otimes e_i|$$

which assigns a normalization factor $\frac{1}{\sqrt{d}}$ to a straight line from the concatenation of a cup and a cap. Furthermore, a projector formed by a top cup and bottom cap forms a representation of the TL algebra. Moreover, quantum teleportation is the

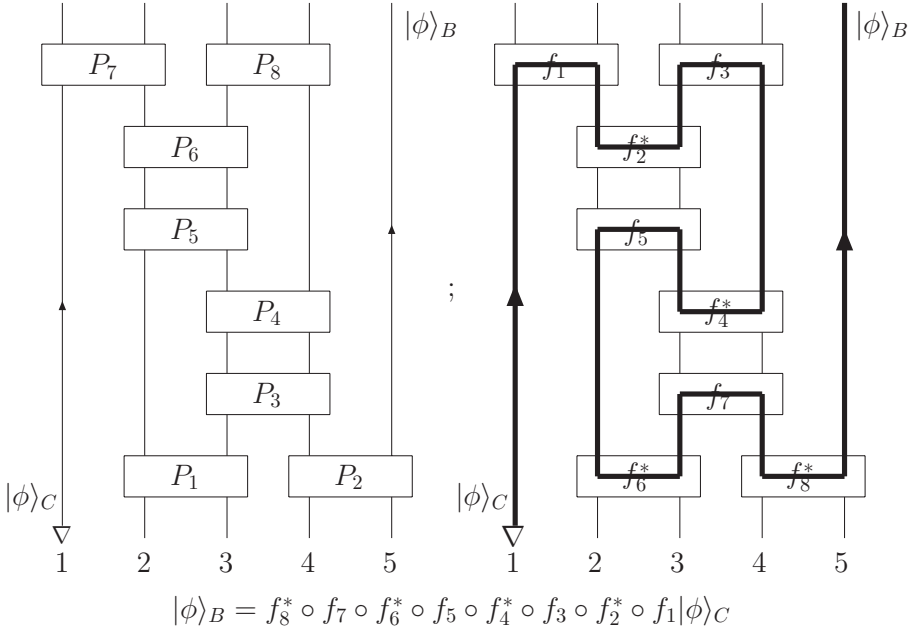


FIGURE 28. Quantum information flow in the categorical approach.

quantum information flow denoted by the topological condition in the teleportation topology, whereas it is described in Figure 16 with the quantum information flow as its part.

7.2. Quantum information flow in terms of maps. Quantum teleportation is an information protocol transporting a unknown quantum state from Charlie to Bob with the help of Alice. To describe it in a unified mathematical formalism, we have to integrate standard quantum mechanics with classical features, since the outcomes of measurements are sent to Bob from Alice via classical channels and then Bob performs a required unitary operation. The categorical approach proposed by Abramsky and Coecke describes the quantum information flow by strongly compact closed categories, see [46, 56, 57].

To sketch the quantum information flow in the form of a composition of a series of maps which are central topics of the category theory, we study an example in detail. Set five Hilbert spaces \mathcal{H}_i and its dual \mathcal{H}_i^* , $i = 1, \dots, 5$, and define eight bipartite projectors $P_\alpha = |\Phi_\alpha\rangle\langle\Phi_\alpha|$, $\alpha = 1, \dots, 8$ in which the bipartite vector $|\Phi_\alpha\rangle$ is an element of $\mathcal{H}_i \otimes \mathcal{H}_{i+1}$, $i = 1, \dots, 4$. In the left diagram of Figure 28, every box represents a bipartite projector P_α , and the vector $|\phi\rangle_C \in \mathcal{H}_1$ that Charlie owns is transported to Bob who obtains the vector $|\phi\rangle_B \in \mathcal{H}_5$ through the quantum information flow. The projectors P_1 and P_2 pick up an incoming vector in $\mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4 \otimes \mathcal{H}_5$, and the projectors P_7 and P_8 determine an outgoing vector in $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4$. The right diagram in Figure 28 shows the quantum information flow from $|\phi\rangle_C$ to $|\phi\rangle_B$. It is drawn according to permitted and forbidden rules [46]: the flow is forbidden to go through a box from the one side to the other side, and is forbidden to be reflected at the incoming point, and has to change its direction

from an incoming flow to an outgoing flow as it passes through a box. Obviously, if these rules are not imposed there will be many possible paths from $|\phi\rangle_C$ to $|\phi\rangle_B$.

Let us set up one-to-one correspondence between a bipartite vector and a map. There are a d_1 -dimension Hilbert space $\mathcal{H}_{(1)}$ and a d_2 -dimension Hilbert space $\mathcal{H}_{(2)}$. The bipartite vector $|\Phi\rangle$ has a form in terms of the product basis $|e_i^{(1)}\rangle \otimes |e_j^{(2)}\rangle$ in $\mathcal{H}_{(1)} \otimes \mathcal{H}_{(2)}$,

$$(107) \quad |\Phi\rangle = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} m_{ij} |e_i^{(1)}\rangle \otimes |e_j^{(2)}\rangle, \quad \langle\Phi| = \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} m_{ij}^* \langle e_i^{(1)}| \otimes \langle e_j^{(2)}|$$

where $\langle\Phi|$ denotes the dual vector of $|\Phi\rangle$ in the dual product space $\mathcal{H}_{(1)}^* \otimes \mathcal{H}_{(2)}^*$ with the basis $\langle e_i^{(1)}| \otimes \langle e_j^{(2)}|$. Besides, once the product basis is fixed, bipartite vectors $|\Phi\rangle$ or $\langle\Phi|$ are determined by a $d_1 \times d_2$ matrix $M_{d_1 \times d_2} = (m_{ij})$. Defining two types of maps f and f^* in the way

$$(108) \quad \begin{aligned} f : \mathcal{H}_1 &\rightarrow \mathcal{H}_2^*, & f(\cdot) &= \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} m_{ij} \langle e_i^{(1)}| \cdot \rangle \langle e_j^{(2)}|, \\ f^* : \mathcal{H}_1^* &\rightarrow \mathcal{H}_2, & f^*(\cdot) &= \sum_{i=0}^{d_1-1} \sum_{j=0}^{d_2-1} m_{ij} |e_j^{(2)}\rangle \langle \cdot | e_i^{(1)} \rangle, \end{aligned}$$

we have the bijective correspondences,

$$(109) \quad |\Phi\rangle \approx \langle\Phi| \approx M \approx f \approx f^*$$

which suggests that the bipartite project box in Figure 28 can be labeled by the map f or f^* or matrix M .

Now we work out the formalism of the quantum information flow in the categorical approach. Consider a projector $P_7 = |\Phi_7\rangle\langle\Phi_7|$ and introduce a map f_1 to represent the action of $\langle\Phi_7|$, a half of P_7 ,

$$(110) \quad f_1 : \mathcal{H}_1 \rightarrow \mathcal{H}_2^*, \quad f_1(\phi_C) = \langle\Phi_7|\phi\rangle_C.$$

Similarly, the remaining seven boxes are respectively labeled by the maps f_2^* , f_3 , f_4^* , f_5 , f_6^* , f_7 and f_8^* , defined by

$$\begin{aligned} f_2^* : \mathcal{H}_2^* &\rightarrow \mathcal{H}_3, & f_2^* \circ f_1(\phi_C) &= \langle\Phi_7|\phi_C \otimes \Phi_6\rangle, \\ f_3 : \mathcal{H}_3 &\rightarrow \mathcal{H}_4^*, & f_3 \circ f_2^* \circ f_1(\phi_C) &= \langle\Phi_7 \otimes \Phi_8|\phi_C \otimes \Phi_6\rangle, \\ f_4^* : \mathcal{H}_4^* &\rightarrow \mathcal{H}_3, & f_4^* \circ f_3 \circ f_2^* \circ f_1(\phi_C) &= \langle\Phi_7 \otimes \Phi_8|\phi_C \otimes \Phi_6 \otimes \Phi_4\rangle, \\ f_5 : \mathcal{H}_3 &\rightarrow \mathcal{H}_2^*, & f_5 \circ f_4^* \circ f_3 \circ f_2^* \circ f_1(\phi_C) &= \langle\Phi_5 \otimes \Phi_7 \otimes \Phi_8|\phi_C \otimes \Phi_6 \otimes \Phi_4\rangle, \\ f_6^* : \mathcal{H}_2^* &\rightarrow \mathcal{H}_3, & f_7 : \mathcal{H}_3 &\rightarrow \mathcal{H}_4^*, & f_8^* : \mathcal{H}_4^* &\rightarrow \mathcal{H}_5, \\ f_6^* \circ f_5 \circ f_4^* \circ f_3 \circ f_2^* \circ f_1(\phi_C) &= \langle\Phi_5 \otimes \Phi_7 \otimes \Phi_8|\phi_C \otimes \Phi_6 \otimes \Phi_4 \otimes \Phi_1\rangle, \\ f_7 \circ f_6^* \circ f_5 \circ f_4^* \circ f_3 \circ f_2^* \circ f_1(\phi_C) &= \langle\Phi_3 \otimes \Phi_5 \otimes \Phi_7 \otimes \Phi_8|\phi_C \otimes \Phi_6 \otimes \Phi_4 \otimes \Phi_1\rangle, \end{aligned}$$

and so the quantum information flow is encoded in the the form

$$(111) \quad \begin{aligned} &f_8^* \circ f_7 \circ f_6^* \circ f_5 \circ f_4^* \circ f_3 \circ f_2^* \circ f_1(\phi_C) \\ &= \langle\Phi_3 \otimes \Phi_5 \otimes \Phi_7 \otimes \Phi_8|\phi_C \otimes \Phi_6 \otimes \Phi_4 \otimes \Phi_1 \otimes \Phi_2\rangle. \end{aligned}$$

Namely, it is a composition of a series of maps,

$$(112) \quad |\phi\rangle_B = f_8^* \circ f_7 \circ f_6^* \circ f_5 \circ f_4^* \circ f_3 \circ f_2^* \circ f_1|\phi\rangle_C$$

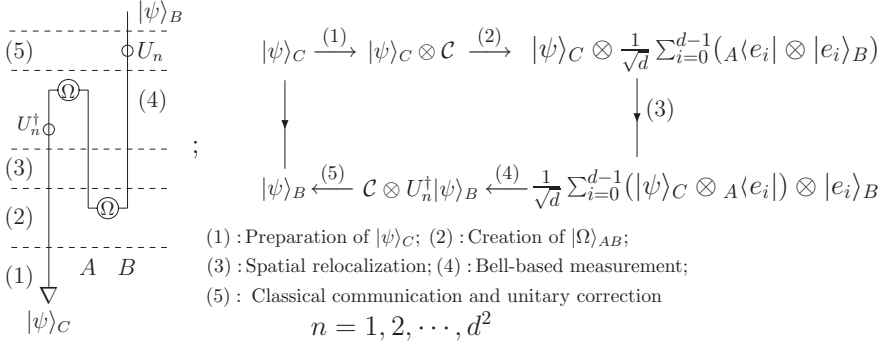


FIGURE 29. Quantum information flow in strongly compact closed categories.

where the tensor product $|\Phi\rangle \otimes \mathbb{I}_d \otimes \dots \otimes \mathbb{I}_d$ is identified with $|\Phi\rangle$. Additionally, following rules of the teleportation topology [13, 29] to assign matrices M, N to a cup and a cap respectively, we have the quantum information flow in the matrix formulation,

$$(113) \quad |\phi\rangle_B = M_8 \cdot N_7 \cdot M_6 \cdot N_5 \cdot M_4 \cdot N_3 \cdot M_2 \cdot N_1 |\phi\rangle_C.$$

The quantum information flow in terms of a composition of maps naturally leads to its description in the category theory. Here we show one-to-one correspondences between the quantum information flow and strongly compact categories. To transport Charlie's unknown quantum state $|\psi\rangle_C$ to Bob, the teleportation has to complete all the operations: the preparation of $|\psi\rangle_C$; the creation of $|\Omega\rangle_{AB}$ in Alice and Bob's system; the Bell-based measurement ${}_{CA}\langle\Omega_n|$ in Charlie and Alice's system; classical communications between Alice and Bob; Bob's local unitary corrections. These steps divide the quantum information flow into six pieces, and they are shown in the left diagrammatical term of Figure 29 where the third piece represents a process bringing Alice and Charlie's systems together for entangling measurement. In the category theory, every step (or piece) is denoted by a specific map satisfying the axioms of strongly compact closed categories. A crucial point is to recognize a bijective correspondence between a Bell state and a map from the dual Hilbert space \mathcal{H}^* to the Hilbert space \mathcal{H} ,

$$(114) \quad \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |e_i\rangle_A \otimes |e_i\rangle_B \approx \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} A\langle e_i| \otimes |e_i\rangle_B, \quad \mathcal{H}_A \otimes \mathcal{H}_B \approx \mathcal{H}_A^* \otimes \mathcal{H}_B$$

so that the quantum information flow have a physical realization in strongly compact closed categories. See the right term of Figure 29: the symbol \mathbb{C} denotes the complex field and

$$(115) \quad |\psi\rangle_C \approx |\psi\rangle_C \otimes \mathbb{C}, \quad |\psi\rangle_B \approx \mathbb{C} \otimes |\psi\rangle_B$$

which suggests a bipartite state is created from vacuum denoted by a complex number and is annihilated it into the vacuum.

7.3. Quantum information flow in the extended TL category. We revisit the example in Figure 28 and redraw a diagram, Figure 30, according to the

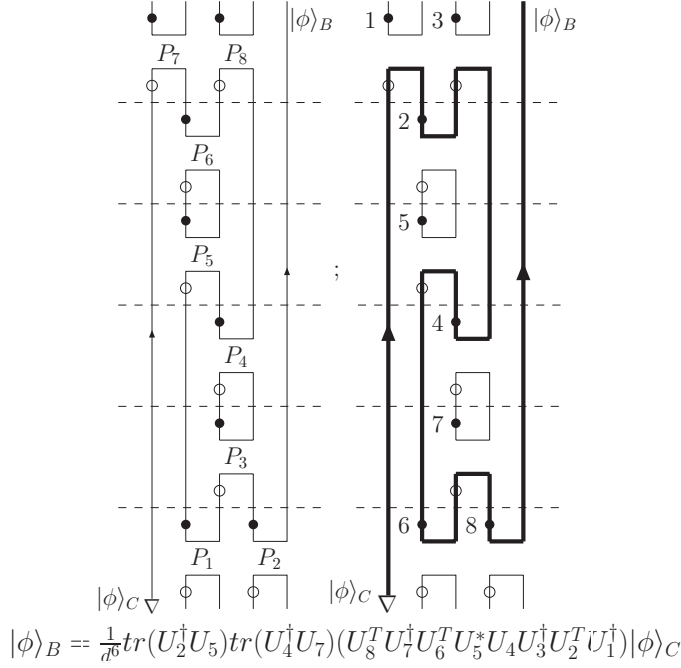


FIGURE 30. Quantum information flow in the extended TL category.

extended TL diagrammatical rules. Every projector consists of a top cup and a bottom cap. Solid points $1, \dots, 8$ on the left branches of cups respectively denote local unitary transformations U_1, \dots, U_8 , and small circles on the left branches of caps denote their adjoint operators $U_1^\dagger, \dots, U_8^\dagger$, respectively. The quantum information flow from $|\phi\rangle_C$ to $|\phi\rangle_B$ is determined by the transfer operator,

$$(116) \quad |\phi\rangle_B = \frac{1}{d^6} \text{tr}(U_2^\dagger U_5) \text{tr}(U_4^\dagger U_7) (U_8^T U_7^\dagger U_6^T U_5^* U_4 U_3^\dagger U_2^T U_1^\dagger) |\phi\rangle_C$$

with the normalization factor $\frac{1}{d^6}$ contributed from six vanishing cups and six vanishing caps as well as two traces from two closed circles.

Five remarks are made as Figure 28 is compared with Figure 30. 1) In the categorical approach, only the half of a projector is exploited to use the bijective correspondence between a bipartite vector and a map to represent the quantum information flow in terms of maps. In the extended TL diagrammatical approach, however, a projector is denoted as the combination of a top cup and a bottom cap instead of a single cup (or cap). Hence the quantum information flow from $|\phi\rangle_C$ to $|\phi\rangle_B$ in Figure 30 has a normalization factor contributed from closed circles which is crucial for the quantum formation flow. For examples, setting eight local unitary operators U_i to be identity leads to $|\phi\rangle_B = \frac{1}{d^6} |\phi\rangle_C$, and assuming U_2 and U_5 (or U_4 and U_7) orthogonal to each other causes a zero vector to be sent to Bob, $|\phi\rangle_B = 0$, no flow! 2) The quantum information flow is only one part of the entire diagram in the extended TL diagrammatical approach. Hence the acausality problem of the quantum information flow in the categorical approach is not reasonable since the whole process is not considered from the global view. 3) In the extended

TL diagrammatical approach, the bijective correspondence between a local unitary transformation and a bipartite vector is considered, which is different from the choice in the categorical approach. For example, we have

$$(117) \quad |\psi(U)\rangle = (U \otimes \mathbb{1}_d)|\Omega\rangle, \quad |\psi(U)\rangle \approx U \approx |\psi(U)\rangle\langle\psi(U)|,$$

and so Bell states (7) are labeled by identity or Pauli matrices

$$(118) \quad |\phi^+\rangle \approx \mathbb{1}_2, \quad |\phi^-\rangle \approx \sigma_3, \quad |\psi^+\rangle \approx \sigma_1, \quad |\psi^-\rangle \approx i\sigma_2.$$

As a projector is labeled by a local unitary transformation, the equation (116) is called the quantum information flow in terms of local unitary transformations (instead of maps). 4) The quantum information flow in the categorical approach is created in view of additional permitted and forbidden rules [46], whereas it is derived in a natural way without imposed rules in the extended TL diagrammatical approach. 5) $\mathcal{H}^* \otimes \mathcal{H}$ is imposed by the axioms of strongly compact closed categories, see Figure 29, but is not required by quantum teleportation, the quantum information flow, and the extended TL category.

8. Concluding remarks

In this paper, we study algebraic structures and low dimensional topology underlying quantum information and computation involving maximally entangled states and local unitary transformations. We describe quantum teleportation from the points of the symmetric group, the braid group, the virtual braid group, the TL algebra and the Brauer algebra, and propose the teleportation swapping, the braid teleportation and the virtual braid teleportation. Especially, quantum teleportation can be performed using the teleportation swapping and Bell measurements, which is a description of quantum teleportation via the Brauer algebra. Besides, we propose the extended TL diagrammatical approach to study a series of topics: the transfer operator with the acausality problem; measurement-based quantum teleportation; tight teleportation and dense coding schemes; the diagrammatical representation of the TL algebra; quantum teleportation and the Brauer algebra; entanglement swapping; universal quantum computing; multipartite entanglements; and quantum information flow. All these examples show that the extended TL category is a mathematical framework describing quantum information and computation using maximally entangled states and local unitary transformations. For example, various descriptions to quantum teleportation can be unified in the extended TL diagrammatical approach.

As a further comment concluding this paper, we remark our previous work [34] on categorical foundation of quantum physics and information. We suggest *unitary Hermitian ribbon categories* as a natural extension of strongly compact closed categories with the extended TL category as its special example. All known diagrammatical approaches [13, 29, 46, 56, 57, 58, 32, 33, 59, 34] to quantum information and computation including the extended TL diagrammatical approach can be viewed as different versions of the diagrammatical representation of tensor categories. Obviously, our future research is focused to look for new quantum information protocols or quantum algorithms with the help of mathematical structures presented in this paper, especially the extended TL category.

Acknowledgements

The author thanks L.H. Kauffman and Y.-S. Wu for helpful comment. He is in part supported by the seed funding of University of Utah and NSFC Grant-10605035.

References

- [1] R.F. Werner, *Quantum States with Einstein-Podolsky-Rosen Correlations Admitting a Hidden-Variable Model*, Phys. Rev. A **40** (1989) 4277.
- [2] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 1999).
- [3] N.D. Mermin, *Quantum Computer Science* (Cambridge University Press, 2007).
- [4] P.W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. In S. Goldwasser, editor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pp. 124-134, Los Alamitos, CA, 1994. IEEE Computer Society Press.
- [5] L.K. Grover, *Quantum Mechanics Helps in Searching for a Needle in a Haystack*, Phys. Rev. Lett. **78** (1997) 325-328.
- [6] C.H. Bennett, G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Int. Conf. Computers, Systems & Signal Processing, Bangalore, India, December 10-12, 1984, pp. 175-179.
- [7] A.K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67** (1991) 661-663.
- [8] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, *Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*, Phys. Rev. Lett. **70** (1993) 1895-1899.
- [9] S.L. Braunstein, G.M. D'Ariano, G.J. Milburn and M.F. Sacchi, *Universal Teleportation with a Twist*, Phys. Rev. Lett. **84** (2000) 3486-3489.
- [10] L.H. Kauffman, *Knots and Physics* (World Scientific Publishers, 2002).
- [11] P.K. Aravind, *Borromean Entanglement of the GHZ state*, in *Potentiality, Entanglement and Passion-at-a-Distance*, R.S. Cohen, M. Horne, and J. Stachel (eds.), pp. 53-59, Kluwer Academic Publishers, Boston 1997.
- [12] H.A. Dye, *Unitary Solutions to the Yang-Baxter Equation in Dimension Four*, Quant. Inf. Proc. **2** (2003) 117-150. Arxiv: quant-ph/0211050.
- [13] L.H. Kauffman and S.J. Lomonaco Jr., *Braiding Operators are Universal Quantum Gates*, New J. Phys. **6** (2004) 134. Arxiv: quant-ph/0401090.
- [14] J.L. Brylinski and R. Brylinski, *Universal quantum gates*, in *Mathematics of Quantum Computation*, Chapman & Hall/CRC Press, Boca Raton, Florida, 2002 (edited by R. Brylinski and G. Chen).
- [15] C.N. Yang, *Some Exact Results for the Many Body Problems in One Dimension with Repulsive Delta Function Interaction*, Phys. Rev. Lett. **19** (1967) 1312-1314.
- [16] R.J. Baxter, *Partition Function of the Eight-Vertex Lattice Model*, Annals Phys. **70** (1972) 193-228.
- [17] Y. Zhang, L.H. Kauffman and M.L. Ge, *Universal Quantum Gate, Yang-Baxterization and Hamiltonian*. Int. J. Quant. Inform., vol. 3, **4** (2005) 669-678. Arxiv: quant-ph/0412095.
- [18] Y. Zhang, L.H. Kauffman and M.L. Ge, *Yang-Baxterizations, Universal Quantum Gates and Hamiltonians*. Quant. Inf. Proc., vol. 4, **3** (2005) 159-197. Arxiv: quant-ph/0502015.
- [19] L.H. Kauffman, *Quantum Computation and the Jones Polynomial*, in *Quantum Computation and Information*, S. Lomonaco, Jr. (ed.), AMS CONM/305, 2002, pp. 101-137. Arxiv: math.QA/0105255.
- [20] L.H. Kauffman, *Quantum Topology and Quantum Computing*, in *Quantum Computation*, S. Lomonaco (ed.), AMS PSAPM/58, 2002, pp. 273-303.
- [21] L. H. Kauffman and S. J. Lomonaco Jr., *Quantum Knots*, in E. Donkor, A.R. Pirich and H.E. Brandt (eds.), *Quantum Information and Computation II*, Spie Proceedings, (12 -14 April, Orlando, FL, 2004), Vol. 5436, pp. 268-284. Arxiv: quant-ph/0403228.
- [22] L.H. Kauffman and S.J. Lomonaco Jr., *Quantum Entanglement and Topological Entanglement*, New J. Phys. **4** (2002) 73.1-73.18.

- [23] L.H. Kauffman and S.J. Lomonaco Jr., *Entanglement Criteria—Quantum and Topological*, in E. Donkor, A.R. Pirich and H.E. Brandt (eds.), *Quantum Information and Computation – Spie Proceedings*, (21-22 April, Orlando, FL, 2003), Vol. 5105, pp. 51-58. Arxiv: quant-ph/0304091.
- [24] Y. Zhang, N. Jing and M.L. Ge, *Quantum Algebras Associated with Bell States*. J.Phys. A: Math. Theor. **41** (2008) 055310.
- [25] J. Franko, E.C. Rowell and Z. Wang, *Extraspecial 2-Groups and Images of Braid Group Representations*. J. Knot Theory Ramifications, **15** (2006) 413-428.
- [26] Y. Zhang and M.L. Ge, *GHZ States, Almost-Complex Structure and Yang–Baxter Equation*. Quant. Inf. Proc. vol. **6**, no. 5, (2007) 363-379.
- [27] Y. Zhang, E.C. Rowell, Y.-S Wu, Z. Wang and M.L. Ge, *From Extraspecial Two-Groups To GHZ States*. Arxiv: quant-ph/0706.1761.
- [28] Y. Zhang, *Quantum Error Correction Code in the Hamiltonian Formulation*. Arxiv: 0801.2561.
- [29] L.H. Kauffman, *Teleportation Topology*. Opt. Spectrosc. **9** (2005) 227-232. Arxiv: quant-ph/0407224.
- [30] R. F. Werner, *All Teleportation and Dense Coding Schemes*, J. Phys. A **35** (2001) 7081–7094. Arxiv: quant-ph/0003070.
- [31] Y. Zhang, L.H. Kauffman and R.F. Werner, *Permutation and its Partial Transpose*. Int. J. Quant. Inform. vol. **5**, no. 4 (2006) 469-507.
- [32] Y. Zhang, *Teleportation, Braid Group and Temperley–Lieb Algebra*. J.Phys. A: Math. Theor. **39** (2006) 11599-11622.
- [33] Y. Zhang, *Algebraic Structures Underlying Quantum Information Protocols*. ArXiv: quant-ph/0601050v2.
- [34] Y. Zhang and L.H. Kauffman, *Topological-Like Features in Diagrammatical Quantum Circuits*, Quant. Inf. Proc. vol. **6**, no. 5 (2007) 477-507.
- [35] H.N.V. Temperley and E.H. Lieb, *Relations between the ‘Percolation’ and ‘Colouring’ Problem and Other Graph-Theoretical Problems Associated with Regular Planar Lattices: Some Exact Results for the ‘Percolation’ Problem*, Proc. Roy. Soc. A **322** (1971) 251-280.
- [36] J.S. Bell, *On the Einstein–Podolsky–Rosen paradox*, Physics **1** (1964) 195-200.
- [37] Y. Aharonov, D.Z. Albert, and L. Vaidman, *Measurement Process in Relativistic Quantum Theory*, Phys. Rev. **D 34** (1986) 1805-1813.
- [38] L. Vaidman, *Teleportation of Quantum States*, Phys. Rev. **A 49** (1994) 1473-1475.
- [39] L. Vaidman, *Instantaneous Measurement of Nonlocal Variables*, Phys. Rev. Lett. **90** (2003) 010402
- [40] L.H. Kauffman, *Virtual Knot Theory*, European J. Comb. **20** (1999) 663-690.
- [41] R. Brauer, *On Algebras Which are Connected With the Semisimple Continuous Groups*, Ann. of Math. **38** (1937) 857-872.
- [42] Y. Zhang, L.H. Kauffman and M.L. Ge, *Virtual Extension of Temperley–Lieb Algebra*. ArXiv: math-ph/0610052
- [43] J. Preskill, *Quantum Information and Computation*, Lecture Notes for Ph219/CS219, Chapter 4, pp. 26-35.
- [44] M. Żukowski, A. Zeilinger, M.A. Horne and A.K. Ekert, *‘Event-Ready-Detectors’ Bell Experiment via Entanglement Swapping*. Phys. Rev. Let. **71** (1993) 4287–4290.
- [45] D. Gottesman and I.L. Chuang, *Quantum Teleportation is a Universal Computational Primitive*. Nature **402** (1999) 390–393. Arxiv:quant-ph/9908010.
- [46] B. Coecke, *The Logic of Entanglement. An Invitation*. Oxford University Computing Laboratory Research Report nr. PRG-RR-03-12. An 8 page short version is at Arxiv:quant-ph/0402014. The full 160 page version is at web.comlab.ox.ac.uk/oucl/publications/tr/rr-03-12.html.
- [47] F. Wilczek, *Fractional Statistics and Anyon Superconductivity* (World Scientific, 1990).
- [48] F.Y. Wu, *Knot Theory and Statistical Mechanics*, Rev. Mod. Phys. **64** (1992) 1099-1131.
- [49] V.F.R. Jones, *Heck Algebra Representations of Braid Groups and Link Polynomials*, Ann. of Math. **126** (1987) 335-388.
- [50] N. Erez, *Teleportation from a Projection Operator Point of View*. Arxiv: quant-ph/0510130.
- [51] P.W. Shor, *Fault-Tolerant Quantum Computation*. In Proceedings, 35th Annual Symposium on Fundamentals of Computer Science (IEEE Press, Los Alamitos, 1996) 56-65. Arxiv: quant-ph/9605011.

- [52] J. Preskill, *Fault-Tolerant Quantum Computation*. Arxiv: quant-ph/9712048.
- [53] D. Aharonov, V. Jones and Z. Landau, *A Polynomial Quantum Algorithm for Approximating the Jones Polynomial*. Arxiv: quant-ph/0511096.
- [54] A. Yu. Kitaev, *Fault-Tolerant Quantum Computation by Anyons*, Annals Phys. **303** (2003) 2-30. Arxiv: quant-ph/9707021.
- [55] M.H. Freedman, M.J. Larsen and Z. Wang, *The Two-Eigenvalue Problem and Density of Jones Representation of Braid Groups*, Comm. Math. Phys. **228** (2002) 177-199.
- [56] S. Abramsky, and B. Coecke, *A Categorical Semantics of Quantum Protocols*. In: Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science (LiCS'04), IEEE Computer Science Press. Arxiv:quant-ph/0402130.
- [57] B. Coecke, *Kindergarten Quantum Mechanics—lecture notes*. In: *Quantum Theory: Reconstructions of the Foundations III*, pp. 81-98, A. Khrennikov, American Institute of Physics Press. Arxiv: quant-ph/0510032.
- [58] R.B. Griffiths, S. Wu, L. Yu and S. M. Cohen, *Atemporal Diagrams for Quantum Circuits*, Phys. Rev. **A 73** (2006) 052309. Arxiv: quant-ph/0507215
- [59] L.H. Kauffman and S.J. Lomonaco Jr., *q-Deformed Spin Networks, Knot Polynomials and Anyonic Topological Quantum Computation*, Arxiv: quant-ph/0606114.

DEPARTMENT OF PHYSICS, UNIVERSITY OF UTAH 115 S, 1400 E, ROOM 201, SALT LAKE CITY, UT 84112-0830

E-mail address: yong@cs.ucf.edu

This page intentionally left blank

Poisson algebras and Yang-Baxter equations

Travis Schedler

Dedicated to Kazem Mahdavi, my kind mentor and friend.

ABSTRACT. We connect generalizations of Poisson algebras with the classical and associative Yang-Baxter equations. In particular, we prove that solutions of the classical Yang-Baxter equation on a vector space V are equivalent to “twisted” Poisson algebra structures on the tensor algebra TV . Here, “twisted” refers to working in the category of graded vector spaces equipped with S_n actions in degree n . We show that the associative Yang-Baxter equation is similarly related to the double Poisson algebras of Van den Bergh. We generalize to L_∞ -algebras and define “infinity” versions of Yang-Baxter equations and double Poisson algebras. The proofs are based on the observation that *Lie* is essentially unique among quadratic operads having a certain distributivity property over the commutative operad; we also give an L_∞ generalization. In the appendix, we prove a generalized version of Schur-Weyl duality, which is related to the use of nonstandard S_n -module structures on $V^{\otimes n}$.

1. Twisted Poisson algebras and the CYBE

Throughout, we will work over a characteristic-zero field \mathbf{k} . The tensor algebra $TV = T_{\mathbf{k}}V$ satisfies the following twisted-commutativity property: each graded component $V^{\otimes m}$ is equipped with an S_m -module structure by permutation of components, and given homogeneous elements $v, w \in TV$ of degrees $|v|, |w|$, we have

$$(1.1) \quad w \otimes v = (21)^{|v|, |w|}(v \otimes w),$$

where $(21)^{|v|, |w|} \in S_{|v|+|w|}$ is the permutation of the two blocks $\{1, \dots, |v|\}, \{|v| + 1, \dots, |v| + |w|\}$. We thus say that TV is a *twisted commutative algebra*.¹

Similarly, we may define twisted Lie algebras. Again let $A = \bigoplus_{m \geq 0} A_m$ together with an S_m action on A_m for all m . A twisted Lie algebra is A together

1991 *Mathematics Subject Classification*. 16W99, 16W35, 16B50.

Key words and phrases. Poisson Algebras, Yang-Baxter equations, Quantum Groups, Category-theoretic methods.

¹The notion of twisted algebras is an old notion from topology dating to at least the 1950’s; see, e.g., [Bar78, Joy86, Fre04, LP06]. They are related to superalgebras and color Lie algebras [RW78, Sch79].

with a graded bracket $\{, \} : A \otimes A \rightarrow A$ satisfying

$$(1.2) \quad \{w, v\} = (21)^{|v|, |w|} \{v, w\},$$

$$(1.3) \quad \{u, \{v, w\}\} + (231)^{|v|, |w|, |u|} \{v, \{w, u\}\} + (312)^{|w|, |u|, |v|} \{w, \{u, v\}\} = 0,$$

where $\sigma = (i_1 i_2 \dots i_n) \in S_n$ denotes the element $\sigma(j) = i_j$, and given $\tau \in S_3$, $\tau^{a, b, c} \in S_{a+b+c}$ denotes the permutation acting by permuting the blocks $\{1, \dots, a\}$, $\{a+1, \dots, a+b\}$, $\{a+b+1, \dots, a+b+c\}$. (We will **not** use cycle notation in this paper.)

The motivating observation of this paper is as follows: If $A = TV$ is endowed with a twisted Lie algebra structure satisfying the Leibniz rule,

$$(1.4) \quad \{u \otimes v, w\} = u \otimes \{v, w\} + (213)^{|v|, |u|, |w|} (v \otimes \{u, w\}),$$

then the Jacobi identity restricted to degree one, $V \otimes V \otimes V \rightarrow T^3 V$, says that the bracket yields a skew solution of the well-known **classical Yang-Baxter equation (CYBE)**:² interpreted as a map $r : V \otimes V \rightarrow V \otimes V$, we have

$$(1.5) \quad r = -r^{21},$$

$$(1.6) \quad [r^{12}, r^{13}] - [r^{23}, r^{12}] + [r^{13}, r^{23}] = 0,$$

where here r^{ij} denotes r acting in the i -th and j -th components (e.g., $r^{23} = \text{Id}_V \otimes r$). The starting point for this paper is then

THEOREM 1.7. *Let V be any vector space. Skew solutions $r \in \text{End}(V \otimes V)$ of the CYBE are equivalent to twisted Poisson algebra structures on TV , equipped with its usual twisted commutative multiplication \otimes .*

Here, a *twisted Poisson* structure on TV is the same as a twisted Lie algebra structure satisfying (1.4).

The proof is based on the twisted generalization of the following well-known fact: a Poisson algebra structure on $\text{Sym } V$ is the same as a Lie algebra structure on V (Proposition 1.10). Precisely, recall that an \mathbb{S} -module is a graded vector space $V = \bigoplus_{m \geq 0} V_m$ together with S_m -actions on each V_m . \mathbb{S} -modules form a symmetric monoidal category, and the notion of $\text{Sym } V$ (the free commutative monoid in the category of \mathbb{S} -modules) makes sense, and yields a twisted commutative algebra. In the case that V is concentrated in degree zero, the twisted commutative algebra $\text{Sym } V$, viewed as an ordinary vector space with the induced multiplication map,³ is the usual symmetric algebra $\text{Sym } V_0$. In the case V is concentrated in degree one, $\text{Sym } V$, viewed as an ordinary vector space with an associative multiplication, is the usual tensor algebra TV_1 .

Then, as explained in §1.1 below, a standard proof that Poisson structures on $\text{Sym } V$ are the same as Lie algebra structures on V carries over to the twisted setting, and yields Theorem 1.7.

REMARK 1.8. P. Etingof pointed out to the author a connection with the Lie algebra \mathfrak{tr} from [BEER05] (which is generated by r_{ij} subject to the universal relations satisfied by r^{ij} for any skew solution r of the CYBE). More precisely,

²The CYBE is a central equation in physics and the study of quantum groups.

³More conceptually, the forgetful functor from \mathbb{S} -modules to vector spaces is a monoidal, although not symmetric monoidal, functor, which is why twisted (commutative or associative) algebras may also be viewed as ordinary associative algebras. These observations have been carried much further in, e.g., [Sto93, PR04].

the universal enveloping algebra of \mathfrak{t} contains the space of all possible operations $V^{\otimes m} \rightarrow V^{\otimes m}$ obtainable from the twisted Lie structure on TV (in terms of an indeterminate r).

1.1. Proof of Theorem 1.7. We recall first the definition of the symmetric monoidal structure on the category of \mathbb{S} -modules: Given \mathbb{S} -modules $V = \bigoplus_{n \geq 0} V_n$ and $W = \bigoplus_{n \geq 0} W_n$,

$$(1.9) \quad (V \otimes W)_p := \bigoplus_{m+n=p} \text{Ind}_{S_m \times S_n}^{S_p} (V_m \otimes W_n).$$

As before, let $\text{Sym } V$ denote the free commutative monoid generated by V , in this category. Theorem 1.7 will follow from the following more general result:

PROPOSITION 1.10. *A multiplication $\{, \} : V \otimes V \rightarrow \text{Sym } V$ satisfying (1.2), (1.3) extends uniquely to a twisted Poisson structure on $\text{Sym } V$.*

In the proof below, it is helpful to have in mind the usual case when V is concentrated in degree zero; here the proof is one of the most obvious ones of the well-known fact that a Lie structure on V extends uniquely to a Poisson structure on $\text{Sym } V$.

We will need to introduce the following notation for technical convenience (and it is not needed in the case V is concentrated in degree zero):

NOTATION 1.11. Given any product of operations applied to symbols x_1, \dots, x_m , which represent elements of degrees $|x_1|, \dots, |x_m|$, let $\sigma'_{x_1, \dots, x_m} \in S_{|x_1| + \dots + |x_m|}$ be the permutation which corresponds to rearranging the symbols in the order x_1, \dots, x_m via a permutation of blocks of sizes $|x_1|, \dots, |x_m|$. For example, in the case $|x_1| = 2, |x_2| = 3$, we have $\sigma'\{x_3, x_2\} = (34512)\{x_3, x_2\}$. Also, let us allow σ' to be extended linearly to linear combinations of such expressions.

PROOF. Uniqueness follows inductively from (1.4). One obtains the formula

$$(1.12) \quad \{v_1 \cdots v_m, w_1 \cdots w_n\} = \sum_{i,j} \sigma'_{v_1, \dots, v_m, w_1, \dots, w_n} (\{v_i, w_j\} v_1 v_2 \cdots \hat{v}_i \cdots v_m w_1 w_2 \cdots \hat{w}_j \cdots w_n).$$

For existence, it suffices to verify the skew-symmetry and Jacobi identity conditions for (1.12). Skew-symmetry is obvious, so it remains to verify the Jacobi identity. This follows inductively from the following computation:

$$(1.13) \quad \begin{aligned} & \sigma'_{a,b,c,d} (\{ab, \{c, d\}\} + \{c, \{d, ab\}\} + \{d, \{ab, c\}\}) \\ &= \sigma'_{a,b,c,d} (b(\{a, \{c, d\}\} + \{c, \{d, a\}\} + \{d, \{a, c\}\}) \\ & \quad + a(\{b, \{c, d\}\} + \{c, \{d, b\}\} + \{d, \{b, c\}\})). \quad \square \end{aligned}$$

PROOF OF THEOREM 1.7. Let W be a vector space and $V := W[1]$ the associated \mathbb{S} -module concentrated in degree one. We showed in Section 1 that the condition that the map $W \otimes W \rightarrow \text{Sym } V \cong TW$ satisfy the twisted skew-symmetry and Jacobi identities is exactly the statement that the associated element $r \in \text{End}(W \otimes W)$ is a skew solution of the CYBE. By Proposition 1.10, we see that under this condition, there is a unique extension to a twisted Poisson structure on $\text{Sym } V \cong TW$. Conversely, any twisted Poisson structure on $TW \cong \text{Sym } V$ restricts to a skew solution $r \in \text{End}(W \otimes W)$ of the CYBE. \square

2. Double Poisson algebras

The author first came upon the aforementioned observations after reading Van den Bergh's paper [VdB04] on double Poisson algebras. These algebras formalize Poisson geometry for noncommutative algebras such as path algebras of quivers (see Example 2.10 below). They are defined by the following axioms, which are quite similar to those for twisted Lie algebras:

DEFINITION 2.1. [VdB04] A double Poisson algebra is an associative algebra A with a \mathbf{k} -linear map $\{\!\!\{ \} \!\!\} : A \otimes A \rightarrow A \otimes A$ satisfying:

$$(2.2) \quad \{\!\!\{ a, b \} \!\!\} = -(21)\{\!\!\{ b, a \} \!\!\},$$

$$(2.3) \quad \sum_{i=0}^2 (231)^i \circ \{\!\!\{ -, \{\!\!\{ -, - \} \!\!\} \} \!\!\} \circ (231)^{-i} = 0,$$

$$(2.4) \quad \{\!\!\{ a, bc \} \!\!\} = (b \otimes 1)\{\!\!\{ a, c \} \!\!\} + \{\!\!\{ a, b \} \!\!\}(1 \otimes c).$$

Dropping the Poisson condition, we define:

DEFINITION 2.5. Let V be any \mathbf{k} -vector space. A double Lie bracket is a \mathbf{k} -linear map $\{\!\!\{ \} \!\!\} : V \otimes V \rightarrow V \otimes V$ satisfying (2.2) and (2.3).

We prove that double Lie algebras are the same as solutions of the associative Yang-Baxter equation (AYBE), which was introduced in [Agu00],[Agu01] and independently in [Pol02]:

$$(2.6) \quad r^{12}r^{13} - r^{23}r^{12} + r^{13}r^{23} = 0.$$

Note that, when r is skew ($r = -r^{21}$), then the AYBE implies the CYBE (this is an special case of [Agu01][Theorem 3.5]). Namely, let $CYBE(r)$ denote the LHS of (1.6) and let $AYBE(r)$ denote the LHS of (2.6). Then, if r is skew, we have

$$(2.7) \quad CYBE(r) = AYBE(r) - (132) \circ AYBE(r) \circ (132).$$

THEOREM 2.8. (i) *Let V be a vector space. Double Lie algebra structures on V are equivalent to skew solutions $r \in \text{End}(V \otimes V)$ of the AYBE. Hence, any double Lie algebra V yields a twisted Poisson algebra structure on $T_{\mathbf{k}}V$ using its tensor product multiplication;*

(ii) *Let A be an associative algebra. Suppose that $r \in \text{End}(A \otimes A)$ satisfies (2.4). If, furthermore, r satisfies the CYBE, then, letting $AYBE(r)$ denote the LHS of (2.6), one has*

$$(2.9) \quad (a \otimes 1 \otimes 1)AYBE(r) = (1 \otimes 1 \otimes a)AYBE(r), \quad \forall a \in A.$$

(iii) *In particular, if A is a prime and noncommutative associative algebra, then (2.9) implies that $AYBE(r) = 0$, so twisted Poisson structures on $T_{\mathbf{k}}A$ satisfying (2.4) (where multiplication is taken in A) are equivalent to double Poisson structures on A .*

In part (iii), “prime” means that, for all nonzero $a, b \in A$, there exists $c \in A$ such that $acb \neq 0$. This is a standard generalization of integral domains to noncommutative rings.

EXAMPLE 2.10. Consider any quiver (= directed graph) Q . We recall that the *path algebra*, $\mathbf{k}Q$, of Q , is the algebra which, as a \mathbf{k} -vector space, is the set of \mathbf{k} -linear combinations of paths in the graph, and whose multiplication is given

by concatenation of paths. To be explicit, we may say that, for paths p and q , pq is the concatenation if the terminal vertex of p equals the initial vertex of q , and otherwise $pq = 0$. This multiplication is extended \mathbf{k} -linearly to all of $\mathbf{k}Q$. If Q is *strongly connected*, which means that for any two vertices i and j , there is a path from i to j , then $\mathbf{k}Q$ is prime. If Q additionally has either at least two vertices or at least two edges, then $\mathbf{k}Q$ is noncommutative. In this case, the theorem shows that double Poisson structures on $\mathbf{k}Q$ are equivalent to twisted Poisson structures on $T_{\mathbf{k}}\mathbf{k}Q$ satisfying (2.4).

We will say that a quiver Q is (extended) Dynkin if the underlying undirected graph (forgetting orientations, but remembering multiplicities) is (extended) Dynkin of type A, D , or E .

EXAMPLE 2.11. For any quiver Q , another important algebra is called the *preprojective algebra* of Q , whose definition we recall as follows. Let $\overline{Q} \supset Q$ be the double quiver, which is the quiver with the same set of vertices as Q , but with twice as many edges: for each edge $e \in Q$, we include not merely e , but add an edge $e^* \in \overline{Q}$ which has the same endpoints as e but points in the opposite direction. Then, Π_Q is defined by $\Pi_Q := \mathbf{k}Q / (\sum_{e \in Q} ee^* - e^*e)$.

Then, by [Sch05, Proposition 9.2.23], for any non-Dynkin quiver Q , Π_Q is prime, and provided $Q \neq \tilde{A}_0$, it is clear that Π_Q is noncommutative. Thus, the theorem applies also to this case.

EXAMPLE 2.12. The deformed preprojective algebra $\Pi_Q^\lambda := \mathbf{k}Q / (\lambda - \sum_{e \in Q} ee^* - e^*e)$ is filtered by degree, and its associated graded is Π_Q . Hence, it is also prime and noncommutative when Π_Q is, and thus the theorem applies.

PROOF OF THEOREM 2.8. (i) Using the obvious correspondence between elements $r \in \text{End}(V \otimes V)$ and double brackets $V \otimes V \rightarrow V \otimes V$, the skew-symmetry condition (2.2) becomes the condition that r is skew. Then, (2.3) becomes

$$(2.13) \quad r^{12}r^{23} + r^{23}r^{31} + r^{31}r^{12} = 0.$$

If we permute the first and third components, multiply by -1 , and apply skew-symmetry, we get (2.6). This proves the first statement. The second statement then follows from the aforementioned fact that the AYBE implies the CYBE for skew elements r .

(ii) Let us write

$$(2.14) \quad AYBE'(r) = r^{13}r^{12} - r^{12}r^{23} + r^{23}r^{13},$$

so that $CYBE(r) = AYBE(r) - AYBE'(r)$. Then, using the derivation property for r , one may verify that

$$(2.15) \quad \begin{aligned} CYBE(r)(a \otimes (b_1 b_2) \otimes c) &= (b_1 \otimes 1 \otimes 1)AYBE(r)(a \otimes b_2 \otimes c) \\ &\quad - (1 \otimes 1 \otimes b_1)AYBE'(r)(a \otimes b_2 \otimes c) + CYBE(r)(a \otimes b_1 \otimes c) \cdot (1 \otimes b_2 \otimes 1), \end{aligned}$$

so that, if $CYBE(r) = 0$, then

$$(2.16) \quad (a \otimes 1 \otimes 1)AYBE(r) = (1 \otimes 1 \otimes a)AYBE'(r), \quad \forall a \in A.$$

However, since $CYBE(r) = 0$, one also has $AYBE(r) = AYBE'(r)$, so

$$(2.17) \quad (a \otimes 1 \otimes 1)AYBE(r) = (1 \otimes 1 \otimes a)AYBE(r), \quad \forall a \in A.$$

(iii) Assume that (2.17) holds. Then,

$$(2.18) \quad (ab \otimes 1 \otimes 1)AYBE(r) = (a \otimes 1 \otimes b)AYBE(r) = \\ (1 \otimes 1 \otimes ba)AYBE(r) = (ba \otimes 1 \otimes 1)AYBE(r).$$

We deduce that $((ab - ba) \otimes 1 \otimes 1)AYBE(r) = 0$. So, if $[A, A]x = 0$ implies $x = 0$ for all $x \in A$, then $AYBE(r) = 0$. This follows because, for arbitrary $y_1, y_2, y_3 \in A$, if we write $AYBE(r)(y_1 \otimes y_2 \otimes y_3) = \sum_i v_i \otimes v'_i$, where the $v'_i \in A \otimes A$ are all linearly independent, and $v_i \in A$, then $((ab - ba) \otimes 1 \otimes 1)AYBE(r) = 0$ implies that $(ab - ba)v_i = 0$ for all i and all a, b . Hence, if $[A, A]x = 0$ implies $x = 0$ for all x , then $v_i = 0$ for all i , and hence $AYBE(r)(y_1 \otimes y_2 \otimes y_3) = 0$. Since $y_1, y_2, y_3 \in A$ were arbitrary, $AYBE(r) = 0$ as well.

On the other hand, to say that $[A, A]a = 0$ implies $a = 0$ is the same as saying that the left ideal generated by $[A, A]$ annihilates only zero. But, the left ideal generated by $[A, A]$ is a two-sided ideal: $w[x, y]z = zw[x, y] + [w[x, y], z]$. So, for $[A, A]a = 0$ to imply $a = 0$, it is enough that $([A, A])a = 0$ implies $a = 0$. If A is prime and noncommutative, then $[A, A]Aa = 0$ implies $a = 0$, hence $([A, A])a = 0$ implies $a = 0$, and so $AYBE(r) = 0$, as desired. \square

REMARK 2.19. One may be curious what happens if A is commutative (such as $\Pi_{\tilde{A}_0}$). In this case, any $r \in \text{End}(A \otimes A)$ satisfying (2.4) satisfies

$$(2.20) \quad (a \otimes 1 - 1 \otimes a)r(b \otimes c) = (c \otimes 1 - 1 \otimes c)r(b \otimes a) = \\ (b \otimes 1 - 1 \otimes b)r(c \otimes a) = (a \otimes 1 - 1 \otimes a)r(c \otimes b),$$

and moreover, for any $a_1, a_2 \in A$,

$$(2.21) \quad (a_1 \otimes 1 - 1 \otimes a_1)(a_2 \otimes 1 - 1 \otimes a_2)r(b \otimes c) = (b \otimes 1 - 1 \otimes b)(c \otimes 1 - 1 \otimes c)r(a_1 \otimes a_2).$$

So this puts special restrictions on r . For instance, if A is a polynomial algebra over a field, then so is $A \otimes A$, and by unique factorization, (2.21) implies that $r(b \otimes c) = (b \otimes 1 - 1 \otimes b)(c \otimes 1 - 1 \otimes c)f = r(c \otimes b)$ for all $b, c \in A$ and some fixed f in the quotient field of $A \otimes A$. (Furthermore, one must have $f \in A \otimes A$ unless A is a polynomial algebra in only one variable x , in which case $f \in (A \otimes A) \cdot (x \otimes 1 - 1 \otimes x)^{-2}$.) Also, for r to be skew, f must be skew, and in this case, the image of r lies in $A \wedge A$, so one deduces that $r^{12}r^{13} = -(213) \circ (r^{12}r^{13}) = r^{12}r^{23} \circ (213)$. In the one-variable case, one deduces that $CYBE(r)(x \otimes x \otimes x) = 0$ iff $AYBE(r)(x \otimes x \otimes x) = 0$, and the latter is true (using the Poisson condition) iff $AYBE(r) = 0$ (and hence $CYBE(r) = 0$). One may then deduce inductively that these are all zero iff $r(x \otimes x) = \lambda(x \otimes 1 - 1 \otimes x)$ for some $\lambda \in \mathbf{k}$. It would be interesting to see if there are other solutions in more variables (and whether AYBE and CYBE have the same solutions). Note that $\Pi_{\tilde{A}_0}$ is the two-variable case.

REMARK 2.22. Many solutions of the AYBE with (graded and spectral) parameters u, v , related to solutions of the CYBE and QYBE, have been classified in [Pol02, Sch03, Pol06]. For example, any “associative Belavin-Drinfeld structure” gives rise to a (trigonometric) such solution which additionally satisfies the QYBE and CYBE with spectral parameters. One may interpret a solution of the AYBE and skew-symmetry (unitarity) with parameters as a sort of graded version of double Lie algebra; to make it Poisson, one would need to find a compatible multiplication (if it exists).

3. Operadic generalization

We ask the question: Is Theorem 1.7 a special property of Lie algebras, or can it be generalized to other operads (suitably replacing the CYBE with other equations)? To make sense of this question, for any twisted-commutative algebra A equipped with an additional binary operation $\star : A \otimes A \rightarrow A$, we generalize the Leibniz rule (1.4) to

$$(3.1) \quad (uv) \star w = u(v \star w) + (213)^{|v|, |u|, |w|} v(u \star w).$$

Let \mathcal{O} be any operad generated by a single element $\mathfrak{m} \in \mathcal{O}(2)$. If A as above is an \mathcal{O} -algebra (with $a \star b := \mathfrak{m}(a \otimes b)$) satisfying (3.1), we call it a *twisted distributive \mathcal{O} -algebra*.

Let \mathcal{F} be the operad freely generated by an element also denoted by $\mathfrak{m} \in \mathcal{F}(2)$. By a quadratic operad $\mathcal{O} = \mathcal{F}/(R)$, we mean one such that $R = R_2 \oplus R_3$, with $R_2 \subset \mathcal{F}(2)$ and $R_3 \subset \mathcal{F}(3)$. In particular, the only possible relations from R_2 are symmetry conditions on \mathfrak{m} , namely, that $(21)\mathfrak{m} = \pm \mathfrak{m}$ as elements of \mathcal{O} . Also, R_3 consists of relations which are quadratic in \mathfrak{m} . We then prove the following result (in §3.1):

DEFINITION 3.2. Let *Lie-adm* denote the Lie-admissible operad, which is the operad whose ordinary algebras are vector spaces together with a binary operation whose skew-symmetrization is a Lie bracket.

THEOREM 3.3. *The only quadratic operads $\mathcal{O} = \mathcal{F}/(R)$ for which distributive \mathcal{O} -algebra structures on $\text{Sym } V$ are equivalent to \mathcal{O} -algebra structures on V , for every vector space V , are the following five:*

- $\mathcal{O} = \text{Lie}$, the Lie operad
- $\mathcal{O} = \text{Lie-adm}$, the Lie-admissible operad
- $\mathcal{O} = \mathcal{F}/(\mathfrak{m} + (21)\mathfrak{m})$, the operad whose algebras are vector spaces with a skew-symmetric binary operation
- $\mathcal{O} = \mathcal{F}/(\mathfrak{m} - (21)\mathfrak{m})$, the operad whose algebras are vector spaces with a symmetric binary operation
- $\mathcal{O} = \mathcal{F}$, the free operad generated by \mathfrak{m} , the operad whose algebras are magmas.

These are also exactly the operads for which twisted distributive \mathcal{O} -algebra structures on $\text{Sym } V$ are equivalent to operations $V \otimes V \rightarrow \text{Sym } V$ satisfying the relations R , for every \mathbb{S} -module V .

After proving this theorem, we will generalize to quadratic operads which are not generated by only a single operation, and find that L_∞ -algebras (heuristically, Lie algebras up to homotopy) are the prototypical example of algebras with operations satisfying the desired distributivity property (Theorem 3.15 and Remark 3.17).

3.1. Proof of Theorem 3.3. As in Proposition 1.10, it is not difficult to show that the listed operads have the desired property. We show the converse. Let \mathcal{F} be as in Theorem 3.1, and let $\mathcal{O} = \mathcal{F}/(R)$ with $R = R_2 \oplus R_3$, where $R_2 \subset \mathcal{F}(2)$ and $R_3 \subset \mathcal{F}(3)$. We show that, if \mathcal{O} -algebra structures on every vector spaces V are equivalent to distributive \mathcal{O} -algebra structures on $\text{Sym } V$, then \mathcal{O} is one of the listed operads.

Assume first that $R_2 = 0$, i.e., there is no (skew)-symmetry axiom for \mathcal{O} -algebras. Take an arbitrary element of R_3 : this is equivalent to a quadratic axiom for \mathcal{O} -algebras (V, \star) . Let us write it as

$$(3.4) \quad \sum_{\sigma \in S_3} \lambda_{\sigma,1} b_{\sigma(1)} \star (b_{\sigma(2)} \star b_{\sigma(3)}) + \lambda_{\sigma,2} (b_{\sigma(1)} \star b_{\sigma(2)}) \star b_{\sigma(3)} = 0,$$

for some constants $\lambda_{\sigma,i}$.

If \mathcal{O} -algebra structures (V, \star) on V are equivalent to distributive \mathcal{O} -algebra structures on $\text{Sym } V$ for all V , then if we expand the above axiom for $(b_1, b_2, b_3) = (b'_1 b''_1, b_2, b_3)$ using the Leibniz rule (3.1), the terms of the form $(x \star y)(z \star w)$ must cancel identically, for $\{x, y, z, w\} = \{b'_1, b''_1, b_2, b_3\}$. That is, the following expression must be identically zero:

$$(3.5) \quad \sum_{\sigma | \sigma(1)=1} \lambda_{\sigma,2} ((b'_1 \star b_2)(b''_1 \star b_3) + (b'_1 \star b_3)(b''_1 \star b_2)) \\ + \sum_{\sigma | \sigma(2)=1} (\lambda_{\sigma,1} + \lambda_{\sigma,2}) ((b_{\sigma(2)} \star b'_1)(b''_1 \star b_{\sigma(3)}) + (b_{\sigma(2)} \star b''_1)(b'_1 \star b_{\sigma(3)})) \\ + \sum_{\sigma | \sigma(3)=1} \lambda_{\sigma,1} ((b_2 \star b'_1)(b_3 \star b''_1) + (b_3 \star b'_1)(b_2 \star b''_1)).$$

This can only happen if the following equations are satisfied:

$$(3.6) \quad \lambda_{\text{id},2} = -\lambda_{(132),2}, \quad \lambda_{(213),2} = -\lambda_{(213),1}, \quad \lambda_{(312),2} = -\lambda_{(312),1}, \quad \lambda_{(231),1} = -\lambda_{(321),1}.$$

Similarly, if we plug in instead

$$(b_1, b_2, b_3) = (b_1, b'_2 b''_2, b_3) \text{ or } (b_1, b_2, b_3) = (b_1, b_2, b'_3 b''_3),$$

we obtain additionally the following conditions:

$$(3.7) \quad \lambda_{(213),2} = -\lambda_{(231),2}, \quad \lambda_{\text{id},2} = -\lambda_{(321),1}, \quad \lambda_{(321),2} = -\lambda_{\text{id},2}, \quad \lambda_{(132),1} = -\lambda_{(312),1}, \\ (3.8) \quad \lambda_{(312),2} = -\lambda_{(321),2}, \quad \lambda_{(132),2} = -\lambda_{(231),1}, \quad \lambda_{(231),2} = -\lambda_{(132),1}, \quad \lambda_{\text{id},1} = -\lambda_{(213),1}.$$

(These can also be obtained from (3.6) by applying the action of S_3 .)

We deduce that the only possible element of R_3 is a multiple of the associated Lie relation, which proves the theorem in the case that $R_2 = 0$.

If $R_2 \neq 0$, then the above computation simplifies. Suppose that R is spanned by $\mathfrak{m} - \varepsilon(21)\mathfrak{m}$ for $\varepsilon \in \{1, -1\}$. Take an arbitrary element of R_3 and write the corresponding axiom for \mathcal{O} -algebras as

$$(3.9) \quad \lambda_1 b_1 \star (b_2 \star b_3) + \lambda_2 b_2 \star (b_3 \star b_1) + \lambda_3 b_3 \star (b_1 \star b_2) = 0.$$

Next, we plug in $b_1 = b'_1 b''_1$ and gather all terms on the LHS of the form $(x \star y)(z \star w)$ where $\{x, y, z, w\} = \{b'_1, b''_1, b_2, b_3\}$:

$$(3.10) \quad \lambda_2 ((b_2 \star b'_1)(b_3 \star b''_1) + (b_2 \star b''_1)(b_3 \star b'_1)) + \lambda_3 ((b_3 \star b'_1)(b'_1 \star b_2) + (b_3 \star b''_1)(b'_1 \star b_2)).$$

The above must be zero, in order for \mathcal{O} to have the desired property. Using the symmetry condition $x \star y = \varepsilon y \star x$, we may rewrite (3.10) as

$$(3.11) \quad (\lambda_2 + \varepsilon \lambda_3) ((b_2 \star b'_1)(b_3 \star b''_1) + (b_3 \star b'_1)(b_2 \star b''_1)).$$

For this to be zero in general, we require that $\lambda_2 = -\varepsilon \lambda_3$. Similarly, setting $(b_1, b_2, b_3) = (b_1, b'_2 b''_2, b_3)$, we conclude that $\lambda_1 = -\varepsilon \lambda_3$, and finally we conclude

that $\lambda_1 = -\varepsilon\lambda_2$. Hence, if $\varepsilon = 1$, then $\lambda_1 = \lambda_2 = \lambda_3 = 0$, and if $\varepsilon = -1$, then $\lambda_1 = \lambda_2 = \lambda_3$ can be arbitrary. This proves the desired result.

For the final statement, it suffices to generalize Proposition 1.10 to the listed operads. This is straightforward and omitted. \square

3.2. L_∞ generalization and arbitrary quadratic operads. In this subsection we will drop the assumption on \mathcal{O} that it be generated by a single binary operation. Suppose instead that \mathcal{O} is generated by any operations, of any arity, satisfying quadratic and linear relations.

The simplest example of this is the case where \mathcal{O} includes a differential $d \in \mathcal{O}(1)$, satisfying $d^2 = 0$. We see that, already, it is not true that $d^2|_V = 0$ implies $d^2|_{\text{Sym } V} = 0$. The solution to this problem is well-known: make V a graded vector space, take d to be an operator of degree -1 , and make $\text{Sym } V$ the supersymmetric algebra generated by V , i.e., $vw = (-1)^{|v||w|}wv$.

It then turns out that Theorems 1.7, 3.3 generalize, roughly, by replacing Lie algebras with L_∞ algebras (heuristically, these are Lie algebra up to homotopy).

We note that the “super” grading above is independent of the twisted grading, so that when one has both, V is bigraded. To simplify things, we restrict to ordinary (not twisted) algebras with a single grading. All of the results generalize to the twisted setting, by working with \mathbb{S} -modules and adding permutations σ' (using Notation 1.11) to the beginning of formulas.

Recall that an L_∞ algebra is a \mathbb{Z} -graded vector space A equipped with a differential $d = \{ \}_1 : A \rightarrow A$ of degree 1, and completely graded-skew-symmetric operations $\{ \}_n : A^{\otimes n} \rightarrow A$ of degrees $2 - n$ (for $n \geq 2$), satisfying axioms (3.12)

$$\sum_{\substack{i+j=m+1, \\ i,j \geq 1}} \sum_{\sigma \in S_m} (-1)^i \text{sign}_{\text{odd}}(\mathbf{a}, \sigma) \{ \{a_{\sigma(1)}, \dots, a_{\sigma(i)}\}_i, a_{\sigma(i+1)}, \dots, a_{\sigma(i+j-1)} \}_j = 0,$$

for all $m \geq 1$, where $\text{sign}_{\text{odd}}(\mathbf{a}, \sigma)$ is the sign of the permutation

$$\sigma^{|a_1|+1, |a_2|+1, \dots, |a_m|+1} \in S_{|a_1|+1+|a_2|+1+\dots+|a_m|+1}$$

obtained from σ by acting on blocks of the sizes $|a_1| + 1, \dots, |a_m| + 1$.

In particular, this includes the axiom that d is a differential, and that the Jacobi identity for $\{ \}_2$ is satisfied up to chain homotopy.

We will use the notation

$$(3.13) \quad \mathbf{b} := (a_1, a_2, \dots, a_{k-1}, a'_k, a''_k, a_{k+1}, \dots, a_m).$$

We define the Leibniz rule for an L_∞ algebra endowed with an additional **super**commutative multiplication as

$$(3.14) \quad \begin{aligned} & \{a_1, a_2, \dots, a_{k-1}, a'_k a''_k, a_{k+1}, \dots, a_m\}_m \\ &= (-1)^{|a'_k|(|a_1|+|a_2|+\dots+|a_{k-1}|)} a'_k \{a_1, a_2, \dots, a_{k-1}, a''_k, a_{k+1}, \dots, a_m\}_m \\ &+ (-1)^{|a''_k|(|a_1|+|a_2|+\dots+|a_{k-1}|+|a'_k|)} a''_k \{a_1, a_2, \dots, a_{k-1}, a'_k, a_{k+1}, \dots, a_m\}_m. \end{aligned}$$

THEOREM 3.15. *An L_∞ structure on $\text{SuperSym } V$ satisfying the Leibniz rule (3.14) is equivalent to operations $\{ \}_i : V^{\otimes i} \rightarrow V$ satisfying the L_∞ axioms (3.12).*

PROOF. This is similar to the proof of Proposition 1.10. We need to show that, given an operation $V \otimes V \rightarrow \text{SuperSym } V$ satisfying the L_∞ axioms (3.12), there is

a unique extension using the Leibniz rule (3.14) to a multiplication $\text{SuperSym } V \otimes \text{SuperSym } V \rightarrow \text{SuperSym } V$, and this also satisfies the L_∞ axioms. The fact that there is a unique extension is easy. To show it satisfies the L_∞ axioms, it is enough inductively to verify that, for any m -tuple of the form $(a_1, a_2, \dots, a_m) = (a'_1 a''_1, a_2, a_3, \dots, a_m) \in (\text{SuperSym } V)^m$, then the L_∞ -axioms for $(a'_1, a_2, a_3, \dots, a_m)$ and $(a''_1, a_2, a_3, \dots, a_m)$ imply the L_∞ axioms for (a_1, a_2, \dots, a_m) . This follows by expanding the expression, for all $m \geq 1$:

$$(3.16) \quad \sum_{i,j:i+j=m+1} \sum_{\sigma \in S_m} (-1)^i \text{sign}(\mathbf{a}, \sigma) \{ \{ a_{\sigma(1)}, \dots, a_{\sigma(i)} \}_i, a_{\sigma(i+1)}, \dots, a_{\sigma(m-1)} \}_j$$

using (3.14), and verifying that the terms of the form $\pm \{ \dots \}_i \cdot \{ \dots \}_j$ cancel. In more detail, it is equivalent to sum above not over all permutations $\sigma \in S_m$, but only over the $i, j - 1$ -shuffles: that is, σ such that $\sigma(\ell) < \sigma(\ell + 1)$ for all $\ell \neq i$ (these are the permutations that leave the order of $1, 2, \dots, i$ and $i + 1, i + 2, \dots, i + j - 1 = m$ unchanged). Then, there is a canonical bijection between $i, j - 1$ shuffles σ such that $\sigma(1) = 1$ and $j, i - 1$ shuffles σ' such that $\sigma'(1) = 1$, and the terms of the form $\pm \{ \dots \}_i \cdot \{ \dots \}_j$ that appear in the expansion of the summand of (3.16) corresponding to (i, j, σ) cancel with the terms of the form $\pm \{ \dots \}_j \{ \dots \}_i$ that appear in the expansion of the summand of (3.16) corresponding to (j, i, σ') . We omit further details. \square

REMARK 3.17. One may obtain a converse of the above theorem, parallel to Theorem 3.3, that is, a description of all $\mathbb{Z}/2$ -graded quadratic operads \mathcal{O} with the super version of the distributivity property of Theorem 3.3 (without the condition that the operad be generated by a single multiplication), using the Leibniz rule (3.14) with $\{ \}_m$ replaced by any m -ary operation corresponding to a generator of \mathcal{O} .

Namely, suppose that the \mathcal{O} is a $\mathbb{Z}/2$ -graded quadratic operad generated by totally graded-skew-symmetric operations o_1, \dots, o_m (with no linear relations aside from that the o_i are graded-skew-symmetric). Then, the distributivity property holds iff the projection of the quadratic relations to the \mathbb{S} -module generated by $o_i \circ (o_j \otimes \text{id}), o_j \circ (o_i \otimes \text{id})$ consists at most of the relation

$$(3.18) \quad \sum_{\sigma \in S_{|o_i|+|o_j|-1}} \text{sign}_{\text{odd}}(\mathbf{a}, \sigma) ((-1)^{|o_i|} \{ \{ a_{\sigma(1)}, \dots, a_{\sigma(|o_i|)} \}_i, a_{\sigma(|o_i|+1)}, \dots, a_{\sigma(|o_i|+|o_j|-1)} \}_j \\ + (-1)^{|o_j|} \{ \{ a_{\sigma(1)}, \dots, a_{\sigma(|o_j|)} \}_j, a_{\sigma(|o_j|+1)}, \dots, a_{\sigma(|o_i|+|o_j|-1)} \}_i) = 0,$$

where $\{ \}_i, \{ \}_j$ denote applying the operations o_i, o_j to the given arguments. The proof is similar to the proofs of Theorems 3.3 and 3.15. If \mathcal{O} is not generated by totally skew-symmetric operations, then the only allowable quadratic relations are those specifying that the skew-symmetrization of the generating operations satisfy certain relations as above. We omit the details.

4. Yang-Baxter-infinity equations and double Poisson-infinity algebras

In view of the fact that L_∞ algebras also have the distributivity property of Theorem 3.3, we explain here the double Poisson analogue of twisted distributive L_∞ structures on TV , which we call “double Poisson-infinity algebras” (Definition

4.1). Here, “infinity” refers to relaxing the Jacobi identity up to higher homotopies: double Poisson-infinity algebras, as we define them, still include an honest associative algebra and the bracket is still skew-symmetric.

Further, using twisted and double Poisson-infinity algebras, we define infinity versions of the classical and associative Yang-Baxter equations (Definition 4.6), by analogy with Theorem 1.7. The CYBE_∞ yields equations for *sequences* of elements $r_n \in \mathfrak{g}^{\otimes n}$ where \mathfrak{g} is any graded Lie algebra, and the AYBE_∞ yields equations for $r_n \in A^{\otimes n}$, where A is any graded associative algebra. We do not know if there exists a corresponding notion of quantum Yang-Baxter equation-infinity.

Specifically, we will (abusively) call a (twisted) commutative and L_∞ algebra satisfying (3.14) a (twisted) “Poisson-infinity” algebra.⁴ As an application of our comparison of twisted and double Poisson algebras, it makes sense to define double Poisson-infinity algebras. To do this, we need only define a “double” version of the Jacobi-infinity identity (3.12). As in the usual setting, we do this by replacing sums over all permutations by sums over only cyclic permutations:

DEFINITION 4.1. A double Poisson-infinity algebra is a \mathbb{Z} -graded associative algebra A together with brackets $\{ \}_n : A^{\otimes n} \rightarrow A^{\otimes n}$ of degree $2 - n$, for all $n \geq 1$, satisfying the identities (for all $n \geq 1$):

(4.2)

Skew-symmetry: $\sigma\{a_{\sigma(1)}, \dots, a_{\sigma(n)}\}_n = \text{sign}(\mathbf{a}, \sigma)\{a_1, a_2, \dots, a_n\}, \forall \sigma \in S_n,$

(4.3) Jacobi $_\infty$:

$$\sum_{\substack{i+j=n+1 \\ n+1}} \sum_{\substack{\sigma \in \\ \mathbb{Z}/(i+j-1)}} (-1)^i \text{sign}_{\text{odd}}(\mathbf{a}, \sigma) \{ \{a_{\sigma(1)}, \dots, a_{\sigma(i)}\}_i, a_{\sigma(i+1)}, \dots, a_{\sigma(i+j-1)} \}_j = 0,$$

(4.4) Double Leibniz: $\{a_1, a_2, \dots, a_{n-1}, a'_n a''_n\}_n$

$$= (-1)^{|a'_n|(|a_1| + \dots + |a_{n-1}|)} a'_n \{a_1, \dots, a_{n-1}, a''_n\}_n + (-1)^n |a''_n| \{a_1, \dots, a_{n-1}, a'_n\}_n a''_n.$$

In a future paper, we hope to explain a double version of Kontsevich’s formal-ity theorem [Kon03], where the above will replace L_∞ for the Poisson side (the differential operator side will use [GS06]).

Finally, we obtain infinity versions of the Yang-Baxter equations by writing down the Poisson-infinity conditions in terms of elements $r_n \in \text{End}(V^{\otimes n})$ (which we may generalize to $\mathfrak{g}^{\otimes n}, A^{\otimes n}$). In order to make the sum over as few terms as possible, and to specialize to the ordinary Yang-Baxter equations, we use the

NOTATION 4.5. Let $Sh_{i,j} \subset S_{i+j}$ denote the set of i, j -shuffles: this means permutations $(k_1 k_2 \dots k_{i+j})$ such that $k_1 < k_2 < \dots < k_i$ and $k_{i+1} < k_{i+2} < \dots < k_{i+j}$.

DEFINITION 4.6. (i) Let \mathfrak{g} be a graded Lie algebra. The **classical Yang-Baxter-infinity equations** for elements $\{r_n \in \mathfrak{g}^{\otimes n}\}_{n \geq 1}$ of degrees $2 - n$ are, for all $n \geq 1$,

$$(4.7) \quad \sum_{i+j=n+1} (-1)^i \sum_{\sigma \in Sh_{i,i+j-1}} [r_i^{\sigma(1), \sigma(2), \dots, \sigma(i)}, r_j^{\sigma(1), \sigma(i+1), \sigma(i+2), \dots, \sigma(i+j-1)}] = 0.$$

⁴This is abusive because this notion of Poisson-infinity only relaxes the Jacobi identity of the bracket, but not the associativity of the multiplication. The operadic notion of Poisson-infinity relaxes both, as well as the Leibniz rule.

(ii) Let A be a graded associative algebra. The **associative Yang-Baxter-infinity equations** for elements $\{r_n \in A^{\otimes n}\}_{n \geq 1}$ of degrees $2 - n$ are, for all $n \geq 1$,

$$(4.8) \quad \sum_{i+j=n+1} (-1)^i \sum_{\sigma \in \mathbb{Z}/n} r_i^{\sigma(1), \sigma(2), \dots, \sigma(i)} r_j^{\sigma(1), \sigma(i+1), \sigma(i+2), \dots, \sigma(i+j-1)} = 0.$$

We remark that the graded condition is not essential for the AYBE_∞ to make sense, although it is needed for CYBE_∞ since we need supercommutators.

It would be interesting to see if there is any reasonable ∞ -analogue of the quantum Yang-Baxter equation, obtained by somehow “quantizing” the above equation.

5. Non-Poisson twisted algebra structures on TV

Let V be a vector space. One interpretation of Theorem 3.3 is that the Leibniz rule (1.4) is not a good condition to impose for many types of algebra structures on TV . For example, the result holds for neither associative algebras nor commutative algebras. In this section, in the form of remarks, we briefly explain how twisted associative algebra structures on TV (*without* the Leibniz condition) are related to the *quantum* rather than the classical Yang-Baxter equation.

Let V be a representation ρ of a Hopf algebra H , which endows $V^{\otimes m}$ (using $\rho^{\otimes m}$) and hence TV with a canonical structure of H -representation. We look for twisted associative algebra structures on TV given by a single element $\mathcal{J} \in H \otimes H$, by the rule

$$(5.1) \quad a \cdot b = \rho^{\otimes |a|} \otimes \rho^{\otimes |b|}(\mathcal{J})(a \otimes b).$$

We obtain the following:

PROPOSITION 5.2. *The formula (5.1) yields a twisted associative algebra structure iff \mathcal{J} is a twist:*

$$(5.3) \quad (\Delta \otimes 1)(\mathcal{J})(\mathcal{J} \otimes 1) = (1 \otimes \Delta)(\mathcal{J})(1 \otimes \mathcal{J}).$$

This has a generalization to algebras over any operad \mathcal{O} , where \mathcal{J} is replaced by an element satisfying an \mathcal{O} -version of (5.3).

We may generalize the above to the case where there is no universal element \mathcal{J} . First, note that the induced multiplication operation on TV is described by the restrictions to $W_1 \otimes W_2 \rightarrow TV$, where W_1, W_2 are irreducible representations of H occurring in TV . This is still true without an element \mathcal{J} . These maps need only satisfy associativity for triples W_1, W_2, W_3 , and preserve a restricted form of the permutation action.

Furthermore, we don’t need to be given an H , since we can always take $H = U(\mathfrak{gl}(V))$. Let $\text{Rep}_{\text{alg}}(\text{End}(V))$ denote the category of algebraic representations of $\text{End}(V)$ viewed as a \mathbf{k} -algebraic monoid, which is equivalent to the category of representations of H occurring in TV . (This includes all representations up to twisting by the trace representation of $\mathfrak{gl}(V)$ (and up to isomorphism).) By Schur-Weyl duality, the S_n action on $V^{\otimes n}$ spans all of $\text{End}_H(V^{\otimes n})$. In the language of category theory, we obtain the

PROPOSITION 5.4. *Twisted associative algebra structures on TV are the same as monoidal structures on the fiber functor $\text{Rep}_{\text{alg}}(\text{End}(V)) \rightarrow \text{Vect}$.*

The above also naturally generalizes to the case of algebra structures on TV that use a modified permutation action, given by an element $R \in \text{End}(V \otimes V)$

(so, $R^{21}R = \text{Id}$ and R satisfies the quantum Yang-Baxter equation, $R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}$). In this case, one has a natural Hopf algebra H_R , defined in [RTF90] (see also the appendix), which makes V a canonical comodule. Using a generalized version of Schur-Weyl duality (Theorem A.7), we obtain the

PROPOSITION 5.5. *Twisted associative algebra structures on (TV, R) are the same as monoidal structures on the fiber functor $\text{Comod}(H_R) \rightarrow \text{Vect}$.*

6. Acknowledgements

The author happened upon the initial discovery in the context of discussions (aimed at [GS06]) with Victor Ginzburg, and he would like to thank Ginzburg for those discussions as well as for encouragement. Thanks are also due to Pavel Etingof and Dimitri Gurevich for useful comments, and to the anonymous referee for many helpful suggestions which improved the exposition. Finally, the author would like to thank K. Mahdavi, D. Koslover, the University of Texas at Tyler, and participants of the 2007 conference in Tyler for the opportunity to communicate this research and interesting discussions. This research was partially supported by an NSF GRF.

Appendix A. Generalized Schur-Weyl duality

A.1. The [RTF90] construction. We recall the definition of the coquasitriangular Hopf algebra H_R . Beginning with any solution R of the QYBE, $R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}$, Faddeev, Reshetikhin, Takhtajan, and Sklyanin [RTF90] constructed the following bialgebra, which is like a R -twisted version of $\mathcal{O}(\text{End}(V))$, the commutative bialgebra of functions on the multiplicative monoid $\text{End}(V)$. It has a coquasitriangular structure from which one recovers R .

DEFINITION A.1. [RTF90] Define H_R to be the quotient of the free algebra $F := \mathbf{k}\langle L_{ij} \rangle_{i,j \in \{1, \dots, n\}}$ by the following relations. Set $L = \sum_{i,j \in \{1, \dots, n\}} e_{ij} \otimes L_{ij} \in \text{End}(V) \otimes F$. Then $H_R := F/I_R$, where I_R is the ideal generated by the relations

$$(A.2) \quad R^{12}L^{13}L^{23} = L^{23}L^{13}R^{12} \in \text{End}(V) \otimes \text{End}(V) \otimes F.$$

We also let L denote its own image under the quotient $F \twoheadrightarrow H_R$. Then, the coproduct Δ and counit ϵ are defined by

$$(A.3) \quad \Delta(L) = L^{12}L^{13}, \quad \epsilon(L) = 1.$$

THEOREM A.4. [RTF90] (cf. [Kas95]) *The preceding definition makes sense and defines a bialgebra (with a unique coquasitriangular structure inducing R).*

By “coquasitriangular structure inducing R ,” we mean a map $H_R \otimes H_R \rightarrow \mathbf{k}$, which satisfies the dual of the quasitriangularity axioms (replacing multiplication by convolution), and whose action on the standard comodule is R . (See [Kas95] for details.)

We will need the standard comodule:

DEFINITION A.5. The “standard comodule” V of H_R is given by the element $L \in \text{End}(V) \otimes H_R \cong \text{Hom}(V, V \otimes H_R)$. That is, the map $\Delta : V \rightarrow V \otimes H_R$ is given by $\Delta(e_j) = \sum_{i=1}^{\dim V} e_i \otimes L_{ij}$. Let $V^{\otimes m}$ denote the comodules obtained by the tensor power of this one.

A.2. Generalized Schur-Weyl duality. In this subsection we prove a generalization of Schur-Weyl duality to the bialgebras H_R . This says that the irreducible subrepresentations of $V^{\otimes m}$ are given by Young diagrams using the R -symmetric action. This result should not be too surprising, given that the relations (A.2) are defined in terms of R , and it is possible that the result even motivated the definition of H_R . However, since the author could not find it in the literature, the result is given here. This result shows that $\text{Comod}(H_R)$ is the same as the category $\mathcal{SW}(V)$ studied in [GM00] (under certain conditions on R).

NOTATION A.6. For any permutation $\sigma \in S_n$, let $\tau_\sigma : V^{\otimes n} \rightarrow V^{\otimes n}$ denote the permutation of components (i.e., the standard permutation action).

THEOREM A.7. Assume $\text{char}(\mathbf{k}) = 0$ and R is a unitary solution of the QYBE. Let $SR_m \subset \text{End}(V^{\otimes m})$ be the image of the R -symmetric action of S_m (generated by elements $\tau_{b,b+1}R^{b,b+1}$), and let $HR_m \subset \text{End}(V^{\otimes m})$ be the span of linear maps of the form $\phi \circ \Delta$, where $\Delta : V^{\otimes m} \rightarrow V^{\otimes m} \otimes H_R$ is the comodule action, and $\phi \in \text{End}(H_R, \mathbf{k})$ is any linear map. Then, one has

$$(A.8) \quad \text{End}_{SR_m}(V^{\otimes m}) = HR_m,$$

$$(A.9) \quad \text{End}_{HR_m}(V^{\otimes m}) = SR_m,$$

$$(A.10) \quad V^{\otimes m} \cong \bigoplus_{\lambda} \rho_{\lambda, S_m} \otimes \rho_{\lambda, H_R},$$

where the sum is over Young diagrams λ parametrizing irreducible representations of S_m , and ρ_{λ, S_m} is the corresponding irreducible representation of S_m . The space ρ_{λ, H_R} is the H_R -subcomodule of $V^{\otimes m}$ equal to $c_\lambda(R)V^{\otimes m}$, where c_λ (cf. [FH91]) is the Young symmetrizer in $\mathbf{k}[S_m]$ corresponding to λ (so that $k[S_m]a_\lambda \cong \rho_{\lambda, S_m}$), and $c_\lambda(R)$ is the corresponding element of $\text{End}(V^{\otimes m})$ given by the “ R -permutation action” $*_R$ of S_m :

$$(A.11) \quad (b, b+1) *_R v := \tau_{(b,b+1)} R^{b,b+1} \cdot v.$$

Furthermore, ρ_{λ, H_R} is an irreducible H_R -comodule, and (A.10) is the multiplicity-free decomposition of $V^{\otimes m}$ into irreducible $SR_m \otimes HR_m$ -modules.

PROOF. We claim that (A.8) is true. First, note that H_R is graded (setting $T_{i,j}$ to have degree 1), and that $\Delta(V^{\otimes m}) \subset V^{\otimes m} \otimes H_R[m]$. Next, consider $HR[1] = F[1]$ to be $\text{End}(V)^*$, by the pairing $(e_{i,j}, T_{k,\ell}) = \delta_{i,k} \delta_{j,\ell}$. This means that $HR[m]^* \subset F[m]^* = \text{End}(V)^{\otimes m}$, which is the subspace respecting the relation (A.2).

Then, the LHS of (A.2), $R^{12}L^{13}L^{23}$, is identified, as a subspace of $\text{End}(V) \otimes \text{End}(V) \otimes F[2] \cong \text{End}(V) \otimes \text{End}(V) \otimes (\text{End}(V)^*)^{\otimes 2}$, with $R^{12}(\text{Id}_{\text{End}(V)}^{13} \text{Id}_{\text{End}(V)}^{24})$, where $\text{Id}_{\text{End}(V)} \in \text{End}(V) \otimes \text{End}(V)^* \cong \text{End}(\text{End}(V))$ is the canonical identity element. Thus, for any $\phi \in \text{End}(V)^{\otimes 2}$, we have

$$(A.12) \quad \phi^{34}(R^{12} \text{Id}_{\text{End}(V)}^{13} \text{Id}_{\text{End}(V)}^{24}) = R\phi \in \text{End}(V \otimes V).$$

Similarly, ϕ^{34} applied to the RHS of (A.2) (considered as an element of $\text{End}(V)^{\otimes 2} \otimes (\text{End}(V)^*)^{\otimes 2}$) is identified with $\phi^{21}R$. So, the condition for ϕ to be an element of $HR[2]^*$ is

$$(A.13) \quad \phi(\tau_{(12)} \circ R) = (\tau_{(12)} \circ R)\phi,$$

which says that ϕ commutes with the R -permutation action. Since H_R is presented by the quadratic relation (A.2), $HR[m]^*$ consists of ϕ that satisfy (A.13) when applying $(\tau_{(12)} \circ R)$ to any components $i, i+1$ for $1 \leq i \leq m-1$. This proves (A.8).

Since S_m is completely reducible over \mathbf{k} (\mathbf{k} has characteristic zero), the above means that $V^{\otimes m}$ decomposes, as a S_m -representation, into a sum of the form

$$(A.14) \quad V^{\otimes m} \cong \bigoplus_{\lambda} \rho_{\lambda, S_m} \otimes V_{m, \lambda, R},$$

where $\rho_{\lambda, S_m} \otimes V_{m, \lambda, R}$ corresponds to the ρ_{λ, S_m} -isotypical part of $V^{\otimes m}$, with respect to the R -permutation action of S_m , and $V_{m, \lambda, R}$ has trivial S_m -action. Then, it immediately follows that $HR_m = \bigoplus \text{Id} \otimes \text{End}(V_{m, \lambda, R})$ with respect to this decomposition, and since the ρ_{λ, S_m} are distinct irreducible representations, (A.9) follows, and hence also (A.10). The remaining statements are immediate, and the theorem is proved. \square

REMARK A.15. The first part of the above theorem, (A.8), is still true if the characteristic of \mathbf{k} is not zero, or if the condition on unitarity is dropped and S_m is replaced by B_m , both using the same proof as above. However, the next two parts may not generalize (since B_m is not finite, its representations are not completely reducible in general, so the double commutant arguments fail). Nonetheless, the inclusion \supseteq in (A.9) is still true and well-known in all cases (i.e., (A.11) defines endomorphisms of comodules).

REMARK A.16. As a special case of the above, we immediately get the usual Schur-Weyl duality for $R = 1$ (and it is essentially the same as Weyl's original proof), except that the usual statement also says that HR_m is generated by the diagonal action of $GL(V)$. To get this last fact, as in Weyl's proof, one may use the fact that the symmetric elements of $W^{\otimes m}$ are generated by the diagonal elements $w^{\otimes m}$, for any vector space W over an infinite field.

References

- [Agu00] M. Aguiar, *Infinitesimal Hopf algebras*, Contemp. Math. **267** (2000), 1–30.
- [Agu01] ———, *On the associative analog of Lie bialgebras*, J. Alg. **244** (2001), no. 2, 492–532.
- [Bar78] M. G. Barratt, *Twisted Lie algebras*, Geometric applications of homotopy theory (Proc. Conf., Evanston, IL, 1977 (Berlin), Lecture Notes in Math., vol. 658, Springer, 1978, pp. 9–15.
- [BEER05] L. Bartholdi, B. Enriquez, P. Etingof, and E. Rains, *Groups and Lie algebras corresponding to the Yang-Baxter equations*, arXiv:math.RA/0509661, 2005.
- [FH91] W. Fulton and J. Harris, *Representation theory. A first course*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, Readings in Mathematics.
- [Fre04] B. Fresse, *Koszul duality of operads and homology of partition posets*, Homotopy theory: relations with algebraic geometry, group cohomology, and algebraic K -theory, Contemp. Math., vol. 346, Amer. Math. Soc., Providence, RI, 2004, math.AT/0301365, pp. 115–215.
- [GM00] D. Gurevich and Z. Mriss, *Schur-Weyl categories and non-quasiclassical Weyl type formula*, Hopf algebras and quantum groups (Brussels, 1998) (New York), Lecture Notes in Pure and Appl. Math., vol. 209, Dekker, 2000, arXiv:math.QA/9911139, pp. 131–158, arXiv:math.QA/9911139.
- [GS06] V. Ginzburg and T. Schedler, *Moyal quantization and stable homology of necklace Lie algebras*, Mosc. Math. J. **6** (2006), no. 3, 431–459, math.QA/0605704.
- [Joy86] A. Joyal, *Foncteurs analytiques et espèces de structures*, Combinatoire énumérative (Montreal, Que., 1985/Quebec, Que., 1985) (Berlin), Lecture Notes in Math., vol. 1234, Springer, 1986, pp. 126–159.
- [Kas95] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, New York, 1995.
- [Kon03] M. Kontsevich, *Deformation quantization of Poisson manifolds*, Lett. Math. Phys. **66** (2003), no. 3, 157–216.

- [LP06] M. Livernet and F. Patras, *Lie theory for Hopf algebras*, arXiv:math.RA/0606329, 2006.
- [Pol02] A. Polishchuk, *Classical Yang-Baxter equation and the A_∞ -constraint*, Adv. Math. **168** (2002), no. 1, 56–95, arXiv:math.AG/0008156.
- [Pol06] ———, *Massey products on cycles of projective lines and trigonometric solutions of the Yang-Baxter equations*, arXiv:math/0612761, 2006.
- [PR04] F. Patras and C. Reutenauer, *On descent algebras and twisted bialgebras*, Mosc. Math. J. **4** (2004), no. 1, 199–216, 311.
- [RTF90] N. Yu. Reshetikhin, L. A. Takhtajan, and L. D. Faddeev, *Quantization of Lie groups and Lie algebras*, Leningrad Math. J. (Algebra i Analiz) **1** (1990), no. 1, 193–225, translated from *Algebra i Analiz* **1** (1989), no. 1, 178–206; alternatively, see *Algebraic Analysis, Vol. I*, 129–139, Academic Press, Boston, MA, 1988.
- [RW78] V. Rittenberg and D. Wyler, *Generalized superalgebras*, Nuclear Phys. B **139** (1978), 189–202.
- [Sch79] M. Scheunert, *Generalized Lie algebras*, J. Math. Phys. (1979), no. 4, 712–720.
- [Sch03] T. Schedler, *Trigonometric solutions of the associative Yang-Baxter equation*, Math. Res. Lett. **10** (2003), no. 2–3, 301–321, arXiv:math.QA/0212258.
- [Sch05] ———, *A Hopf algebra quantizing a necklace Lie algebra canonically associated to a quiver*, Int. Math. Res. Not. (2005), no. 12, 725–760, IMRN/14217.
- [Sto93] C. R. Stover, *The equivalence of certain categories of twisted Lie and Hopf algebras over a commutative ring*, J. Pure Appl. Algebra **86** (1993), no. 3, 289–326.
- [VdB04] M. Van den Bergh, *Double Poisson algebras*, math.QA/0410528, 2004.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CHICAGO, 5734 S. UNIVERSITY AVE, CHICAGO IL 60637, USA

E-mail address: `trasched@math.uchicago.edu`

Ambiguity in quantum-theoretical descriptions of experiments

John M. Myers and F. Hadi Madjid

ABSTRACT. This paper contributes to a burgeoning area of investigation, the ambiguity inherent in mathematics and the implications for physics of this ambiguity. To display the mathematical form of equations of quantum theory used to describe experiments, we make explicit the knobs by which the devices of an experiment are arranged and adjusted. A quantum description comes in two parts: (1) a statement of results of an experiment, expressed by probabilities of detections as functions of knob settings, and (2) an explanation of how we think these results come about, expressed by linear operators, also as functions of knob settings. Because quantum mechanics separates the two parts of any description, it is known that between the statements of results and the explanations lurks a logical gap: given any statement of results one has a choice of explanations.

Here we work out some consequences of this openness to choice. We show how quantum theory as mathematical language in which to describe experiments necessarily involves multiple descriptions: multiple explanations of a given result, as well as multiple statements of results and multiple arrangements of knobs. Appreciating these multiplicities resolves what otherwise is a confusion in the concept of invariance. Implications of multiplicity of description for the security of quantum key distribution are noted.

1. Introduction

Quantum theory can be used as a language in which to speak mathematically of particles and fields or, and this is our focus, as a language in which to describe experiments with devices, such as lasers and lenses and detectors on a laboratory bench. To employ quantum theory as mathematical language to describe experiments with devices, one assumes that the devices generate, transform, and measure particles and/or fields, expressed one way or another as linear operators. We omit discussing how one arrives at the particles, or even whether one takes them as observable or as imaginative constructs; instead we attend directly to the linear operators that end up expressing the devices. These operators are functions of the parameters by which one describes control over the devices. By making explicit the parameters that express the knobs and levers that control an experiment, we will

1991 *Mathematics Subject Classification.* 60B05, 81Q99.

Key words and phrases. quantum theory, ambiguity, probability, operator.

show how quantum theory as mathematical language in which to describe experiments forces multiple descriptions. We will also show a few of the consequences of this multiplicity.

It is important to recognize that quantum theoretic descriptions of experiments come in two parts: (1) statements of results of an experiment, expressed by probabilities of detections as functions of knob settings, and (2) explanations of how one thinks these results come about, also as functions of knob settings. Given an explanation in terms of linear operators, one knows from the trace rule how to calculate the probabilities that constitute a statement of results. We will attend as much, if not more, to the “inverse problem” of choosing linear operators to explain given probabilities. When we want to create an explanation in operators of a given statement of results, these results together with the rules of linear operators act as an axiom system. From the standpoint of logic, an explanation is an interpretation of the results. Going back at least to Hilbert’s bizarre interpretations of the axioms of geometry, there is a developing awareness that mathematics is ambiguous, and that this ambiguity is no fault to be repaired, but is intrinsic to mathematics and indeed to “language itself” [1].

A few years ago we proved that between the two parts of a description—the statement of results and the explanation—lurks a gap not bridged by logic, open to choice resolvable only by stepping outside logic to make an assumption that, inspired or not, can be called a guess [2]–[5]. The proof prompts further exploration, and here we report on: (1) implications of statements of results for the topology of knobs, *independent of choices of explanation*; (2) an endless cycle of extensions of both explanations and statements of results forced by openness to choice; and (3) an apparent paradox in the concept of invariance, resolved by recognizing multiple descriptions. Along the way we note implications of ambiguities of description for quantum cryptography. A take-home lesson is that descriptions expressed in quantum theory make sense only in a context of more than one description, so that relations among different descriptions—both the statements of results and their explanations—become essential ingredients in the very concept of a description.

Note that while our discussion gives knobs a prominent expression absent in text books on quantum mechanics, we employ the standard quantum mechanics of Dirac and von Neumann [6, 7], augmented only by positive-operator-valued measures, now in widespread use.

2. Lattices of domains of knobs and detectors

To display the dependence of quantum explanations on choices, we need first to say how to express *knobs* in the mathematical language in which we describe experimental trials, actual or anticipated. As already noted, the mathematics used to describe trials of an experiment partitions into a statement of results and an explanation, both of which depend on the knobs and levers by which one controls devices arranged into an experiment. Subsuming levers into knobs, we express any one knob by a set of *settings* of the knob. Later we will see topologies and metrics for some knobs but for the moment we take knobs just as sets. A knob depends on a level of description; what in a coarse description is “a knob” splits in some finer description into several knobs. (This ambiguity reflects the ambiguity of what to call an “element of a set”; *i.e.* an element of one set can itself be a set.)

To permit describing a given experiment at differing levels of detail and to describe several related experiments that overlap in their knobs, we introduce a lattice structure for sets of knobs (and later also a lattice for sets of detectors). We define a *knob domain* in terms of an *unordered* product of knobs, as discussed in Appendix A. Knob domains are partially ordered by the knobs they include. Given two knob domains \mathbf{K} and \mathbf{K}' , we can form their *meet* $\mathbf{K} \wedge \mathbf{K}'$ (the knobs they share in common) and their *join* $\mathbf{K} \vee \mathbf{K}'$ (combining all the knobs involved in either), so that knob domains form a distributive lattice. When a knob domain \mathbf{K} is an unordered product of several knobs, then an element $k \in \mathbf{K}$ specifies a particular setting for each of the knobs of \mathbf{K} .

A detector is expressed mathematically by a set Ω of possible outcomes. We allow for continuous detector responses by dealing with $\tilde{\Omega}$, a σ -algebra of measurable subsets of a detector Ω . Just as experiments can have multiple knobs, leading to the notion of a knob domain, they can have multiple detectors, again expressed by unordered products. We call unordered products of detectors *detector domains*. Detector domains $\tilde{\Omega}, \tilde{\Omega}', \dots$ form a lattice, as described in Appendix A.

3. Statements of results and explanations

Given a lattice of knob domains and a lattice of detector domains, let PPM denote the function that assigns to each knob domain \mathbf{K} and each detector domain $\tilde{\Omega}$ the set of parametrized probability measures over that pair of domains:

$$(1) \quad \text{PPM}(\mathbf{K}, \tilde{\Omega}) \stackrel{\text{def}}{=} \{\mu | \mu: \mathbf{K} \times \tilde{\Omega} \rightarrow [0, 1]\},$$

subject to the condition:

$$(2) \quad (\forall k \in \mathbf{K}) \quad \mu(k, -): \tilde{\Omega} \rightarrow [0, 1] \text{ is a probability measure on } \tilde{\Omega}.$$

For any given knob and outcome domains, a statement of results is some $\mu \in \text{PPM}(\mathbf{K}, \tilde{\Omega})$.

3.1. Metric deviation of two parametrized probability

measures. Here are two ways to compare parametrized probability measures. Let $\text{PrMeas}(\tilde{\Omega})$ denote the set of probability measures on $\tilde{\Omega}$. For any detector domain $\tilde{\Omega}$, the Euclidean bounded metric on $[0, 1]$ lifts to the uniform metric D_{Ω} on $\text{PrMeas}(\tilde{\Omega})$; that is for any $\nu, \nu' \in \text{PrMeas}(\tilde{\Omega})$ we have

$$(3) \quad D_{\Omega}(\nu, \nu') \stackrel{\text{def}}{=} \sup_{\omega \in \tilde{\Omega}} |\nu(\omega) - \nu'(\omega)| = \sup_{\omega \in \tilde{\Omega}} [\nu(\omega) - \nu'(\omega)],$$

where the absolute value can be dropped because a measure space is closed under complements. Applied to compare a single parametrized probability measure evaluated at two values $k_1, k_2 \in \mathbf{K}$, we have

$$(4) \quad D_{\Omega}[\mu(k_1, -), \mu(k_2, -)] = \sup_{\omega \in \tilde{\Omega}} [\mu(k_1, \omega) - \mu(k_2, \omega)].$$

A second lift puts the uniform metric on parametrized probability measures: for $\mu_1, \mu_2 \in \text{PPM}(\mathbf{K}, \tilde{\Omega})$

$$(5) \quad D_{\mathbf{K}, \Omega}(\mu_1, \mu_2) \stackrel{\text{def}}{=} \sup_{k \in \mathbf{K}} \sup_{\omega \in \tilde{\Omega}} [\mu_1(k, \omega) - \mu_2(k, \omega)];$$

however a coarser way of comparing functions from sets to topological spaces can be applied across different topological spaces, and for our purpose this is the more

useful comparison. With apologies to whomever knows it by another name, we call it “metric deviation” and define it in Appendix B. For μ and μ' having the same knob domain \mathbf{K} but possibly distinct detector domains $\tilde{\Omega}$ and $\tilde{\Omega}'$, respectively, we define

$$(6) \quad \text{MetDev}(\mu, \mu') \stackrel{\text{def}}{=} \sup_{k_1, k_2 \in \mathbf{K}} |D_{\tilde{\Omega}}[\mu(k_1, -), \mu(k_2, -)] - D_{\tilde{\Omega}'}[\mu'(k_1, -), \mu'(k_2, -)]|.$$

An application of this metric deviation is described in Sec. 4.

3.2. Explanations. Besides stating results there is *explaining* them. A quantum explanation of a statement of result $\mu: \mathbf{K} \times \tilde{\Omega} \rightarrow [0, 1]$ consists of linear operators on some Hilbert space \mathcal{H} as functions of the knob settings, including detection operators involving $\tilde{\Omega}$. Products, tensor products, sums, exponentiations, etc. of operators are combined to form a triple (\mathcal{H}, ρ, M) in which ρ and M are functions on \mathbf{K} . The function $\rho: \mathbf{K} \rightarrow \{\text{density operators on } \mathcal{H}\}$ can be called a parametrized density operator, and the function $M: \mathbf{K} \times \tilde{\Omega} \rightarrow \{\text{Detection operators on } \mathcal{H}\}$ is a parametrized positive operator-valued measure (POVM); more precisely, for each $k \in \mathbf{K}$, $M(k, -): \tilde{\Omega} \rightarrow \{\text{Detection operators on } \mathcal{H}\}$ is a POVM on the measurable sets of $\tilde{\Omega}$. So defined, any explanation implies a statement of results *via* the familiar trace rule

$$(7) \quad (\forall k \in \mathbf{K}, \omega \in \tilde{\Omega}) \quad \mu(k, \omega) = \text{Tr}_{\mathcal{H}}[\rho(k)M(k, \omega)],$$

where $\omega \in \tilde{\Omega}$ is an outcome. Often we abbreviate this by

$$(8) \quad \mu = \text{Tr}_{\mathcal{H}}[\rho M].$$

Let Expl denote the function that assigns to each knob domain \mathbf{K} and each detector domain $\tilde{\Omega}$ the set of explanations over those domains:

$$(9) \quad \text{Expl}(\mathbf{K}, \tilde{\Omega}) \stackrel{\text{def}}{=} \{(\mathcal{H}, \rho, M)\},$$

subject to the conditions:

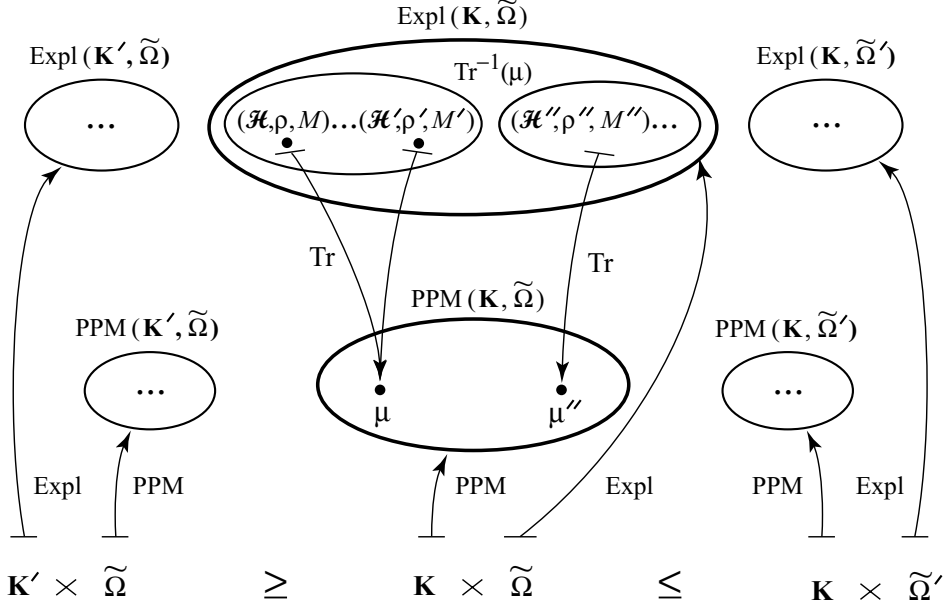
- (1) $\rho: \mathbf{K} \rightarrow \{\text{density operators on } \mathcal{H}\}$ and
- (2) $(\forall k \in \mathbf{K}) M(k, -): \tilde{\Omega} \rightarrow \{\text{Detection operators on } \mathcal{H}\}$ is a POVM on $\tilde{\Omega}$.

For any such explanation, $\text{Tr}_{\mathcal{H}}[\rho M] \in \text{PPM}(\mathbf{K}, \tilde{\Omega})$.

3.3. Choice of explanation. Now comes the inverse problem, with its non-uniqueness. Given a statement of results in the form of a given parametrized probability measure μ , what freedom of choice is there for an explanation (\mathcal{H}, ρ, M) that generates this μ ? Part of the answer comes as a proof of a logical ambiguity—not a break or a conflict, but a place for choice: no matter what probabilities are given as functions of knob settings, there is always room for choice of ρ and M [2, 4, 5].

Although we barely touch on them in this paper, mappings between domains $\mathbf{K} \times \tilde{\Omega}$ and domains $\mathbf{K}' \times \tilde{\Omega}'$ induce mappings from $\text{PPM}(\mathbf{K}', \tilde{\Omega}')$ to $\text{PPM}(\mathbf{K}, \tilde{\Omega})$; likewise mappings on domains induce mappings between explanations on the respective domains. If we view explanations and statements of results as two categories, the trace respects the mappings we have in mind, and so acts as a functor from explanations to statements of results. This functor is full but unfaithful.

Choices of explanations for a given statement of results arise because the trace as a functor from explanations to statements of results has a “roomy inverse,” as illustrated in Fig. 1. Given $\mu \in \text{PPM}(\mathbf{K}, \tilde{\Omega})$, the inverse image $\text{Tr}^{-1}(\mu) \subset$


 FIGURE 1. $\text{Tr}^{-1}(\mu)$ contains many explanations.

$\text{Expl}(\mathbf{K}, \tilde{\Omega})$ is a big set involving an infinite tower of Hilbert spaces and generically including explanations that, as we shall see, have diverse implications.

3.4. Metric deviations of explanations. The concept of metric deviation, introduced above, can be applied not only to parametrized probability measures but also to parametrized density operators and parametrized POVMs. These metric deviations of operator-valued functions of knobs allow comparisons of explanations finer-grained than a comparison of their traces; unlike operator metrics for operators on a given Hilbert space, the metric deviations allow comparisons of operators on distinct Hilbert spaces. To define the metric deviations, we first recall metrics for operators that share a common Hilbert space. Because of its role in quantum decision theory, the trace distance is the most suitable metric for positive trace-class operators, including density operators. For $\rho: \mathbf{K} \rightarrow \text{DensOp}(\mathcal{H})$ the trace distance between $\rho(k_1)$ and $\rho(k_2)$ is $\frac{1}{2}\text{Tr}_{\mathcal{H}}|\rho(k_1) - \rho(k_2)|$ [8]. For ρ and ρ' defined on the same domain \mathbf{K} but with codomains $\text{DensOp}(\mathcal{H})$ and $\text{DensOp}(\mathcal{H}')$, respectively, where the Hilbert space \mathcal{H} need not be the same or even isomorphic to \mathcal{H}' , we define a metric deviation by

$$(10) \quad \text{MetDev}(\rho, \rho') \stackrel{\text{def}}{=} \sup_{k_1, k_2 \in \mathbf{K}} \left| \frac{1}{2}\text{Tr}_{\mathcal{H}}|\rho(k_1) - \rho(k_2)| - \frac{1}{2}\text{Tr}_{\mathcal{H}'}|\rho'(k_1) - \rho'(k_2)| \right|.$$

For POVMs, the trace need not exist, and we invoke the metric derived from the norm $\|\cdot\|_{\mathcal{H}}$ for operators on a Hilbert space \mathcal{H} [9]. For two POVMs with detection operators for outcomes in $\tilde{\Omega}$ on \mathcal{H} , the norm $\|\cdot\|_{\mathcal{H}}$ permits defining a uniform metric, in which the distance between $M(k_1, -)$ and $M(k_2, -)$ is $\sup_{\omega \in \tilde{\Omega}} \|M(k_1, \omega) - M(k_2, \omega)\|_{\mathcal{H}}$. Although in this paper we make no use of it, we define a metric deviation for POVMs M and M' that share the same knob domain \mathbf{K} but can differ

in both their Hilbert spaces and their detector domains as:

$$\text{MetDev}(M, M') \stackrel{\text{def}}{=} \sup_{k_1, k_2 \in \mathbf{K}} \left| \sup_{\omega \in \tilde{\Omega}} \|M(k_1, \omega) - M(k_2, \omega)\|_{\mathcal{H}} - \sup_{\omega' \in \tilde{\Omega}'} \|M'(k_1, \omega') - M(k_2, \omega')\|_{\mathcal{H}'} \right|. \quad (11)$$

4. Topologies and metrics induced on knobs by detections

The diversity of explanations available for any given statement of results prompts the question: what can we learn about knobs just from detection results μ , without invoking any of the explanations in $\text{Tr}^{-1}(\mu)$? So far knob domains have lacked topology. As outlined in Appendix B.1, for any set \mathbf{K} , a function from \mathbf{K} to a metric space induces a topology on \mathbf{K} . Now probability measures on $\tilde{\Omega}$ come with the uniform bounded metric D_{Ω} defined in Eq. (3). View any parametrized probability measure μ as a function $\mu: \mathbf{K} \rightarrow \text{PrMeas}(\tilde{\Omega})$, where \mathbf{K} is taken as a set, without any assumption of a topology, and $\text{PrMeas}(\tilde{\Omega})$ has the metric topology induced by D_{Ω} . For $V \subset \text{PrMeas}(\tilde{\Omega})$, define $\mu^{-1}(V) \stackrel{\text{def}}{=} \{k \in \mathbf{K} | \mu(k, -) \in V\}$. Per Appendix B.1, μ induces a topology on \mathbf{K} specified by

$$(12) \quad \tau_{\mu} = \{U \subset \mathbf{K} | (\exists V \text{ open in } \text{PrMeas}(\tilde{\Omega})) \quad U = \mu^{-1}(V)\}.$$

If μ is an injection into $\text{PrMeas}(\tilde{\Omega})$, then the (bounded) uniform metric on $\text{PrMeas}(\tilde{\Omega})$ induces a bounded metric on \mathbf{K} . If it is not injective, then μ induces a bounded metric on the quotient set of equivalence classes \mathbf{K}/E_{μ} where E_{μ} is the equivalence relation defined by

$$(13) \quad k_1 E_{\mu} k_2 \Leftrightarrow \mu(k_1, -) = \mu(k_2, -).$$

Examples of equivalence classes of knobs relevant to entangled states are discussed in [5], where they are level sets relevant to entangled states that violate Bell inequalities. When μ is not injective, in many cases the coarse topology τ_{μ} on \mathbf{K} induced by μ can be replaced by a finer topology by recognizing a finer level of description that augments the detector domain by adding another detector, as discussed below in connection with equivalence classes that characterize invariance.

Remark: Consider two parametrized probability measures μ and μ' having the same knob domain \mathbf{K} but possibly distinct detector domains $\tilde{\Omega}$ and $\tilde{\Omega}'$, respectively. If their metric deviation is zero, then Appendix B.1 shows they induce the same topological and metric structures on \mathbf{K} .

$$(14) \quad \text{MetDev}(\mu, \mu') = 0 \Rightarrow \tau_{\mu} = \tau_{\mu'}.$$

5. Inequivalent explanations force extensions of domains

Although ambiguities preclude logic from forcing a single explanation, the existence of ambiguity logically forces a dynamic that continually extends statements of results and explanations. Picture a “penguin” toy walking down a slope with a rolling gait, leaning left and swinging its right leg, then leaning right and swinging its left leg, on and on in a cycle. From the proofs in [4] and the lattice structure

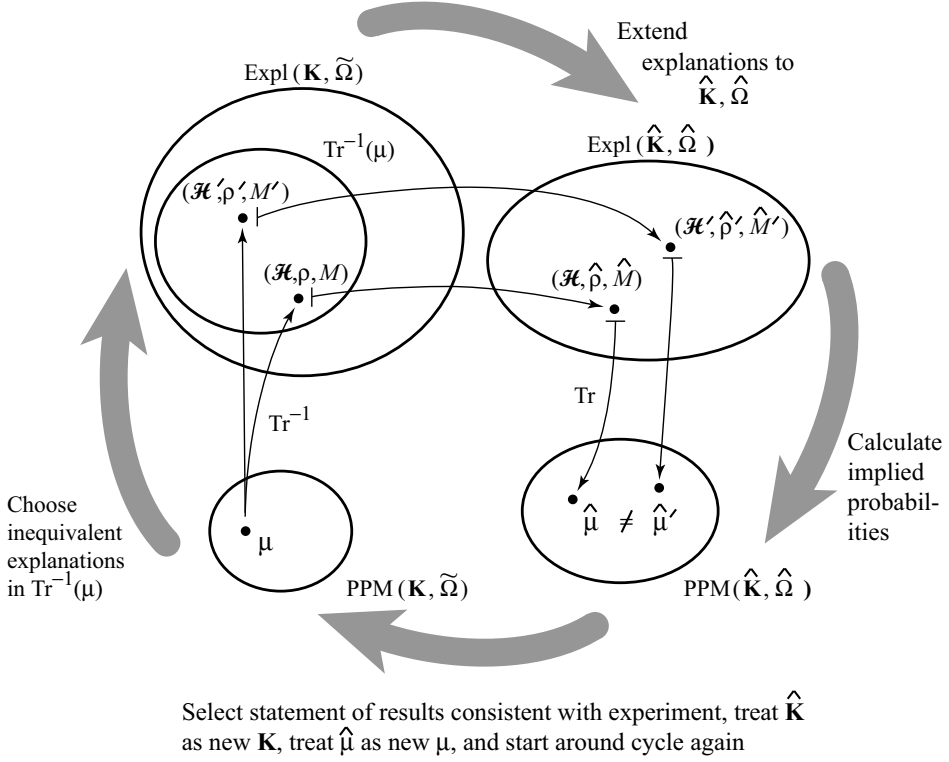


FIGURE 2. Expanding cycle of results and explanations.

of knob domains and detector domains follows the openness of a cycle of stating experimental results and explaining these results, as illustrated in Fig. 2. This cycle operates in a context not limited to theory but including the experimental endeavors that theory describes. While here we cannot reach beyond quantum formalism to touch them, we have experiments in mind as a background against which a statement of results implied by an explanation can be judged and, if incompatible, rejected.

Here is how the expanding cycle works. Given any \mathbf{K} of more than one element and a generic $\mu: \mathbf{K} \rightarrow \text{PrMeas}(\tilde{\Omega})$ there are explanations $(\mathcal{H}, \rho, M), (\mathcal{H}', \rho', M') \in \text{Tr}^{-1}(\mu)$ with the property that $\text{MetDev}(\rho, \rho') \neq 0$ [4]; without loss of generality suppose that

$$(15) \quad \frac{1}{2} \text{Tr}_{\mathcal{H}} |\rho(k_1) - \rho(k_2)| > \frac{1}{2} \text{Tr}_{\mathcal{H}'} |\rho'(k_1) - \rho'(k_2)|.$$

Suppose the explanation is expanded to cover a larger knob domain in such a way that the density operator and the POVM can be independently selected. Leaving the choice of density operators unchanged, consider the effect of the availability of certain additional POVMs as expressed by expanding the domain of knobs from \mathbf{K} to $\hat{\mathbf{K}} = \mathbf{K} \vee \mathbf{L}$ where \mathbf{L} comprises a copy of \mathbf{K} and, in addition, an extra knob domain \mathbf{B} . The explanations expand to $(\mathcal{H}, \hat{\rho}, \hat{M}), (\mathcal{H}', \hat{\rho}', \hat{M}')$ in which the POVMs \hat{M} and \hat{M}' are functions on $\mathbf{L} \cong \mathbf{K} \vee \mathbf{B}$. We design one setting $b_0 \in \mathbf{B}$ to work so that $(\forall k \in \mathbf{K})$ the setting $(k, k, b_0) \in \hat{\mathbf{K}}$ has the same effect as does

$k \in \mathbf{K}$; that is, the expanded explanations envelop the given explanations by the mappings

$$(16) \quad \hat{M}(k, b_0, -) = M(k, -),$$

$$(17) \quad \hat{M}'(k, b_0, -) = M'(k, -).$$

Correspondingly, the statements of results implied by the explanations are also enveloped [5] by the larger domain under the condition that $b = b_0$, in that we have ($\forall k \in \mathbf{K}$)

$$(18) \quad \begin{aligned} \hat{\mu}(k, k, b_0, \omega) &= \text{Tr}_{\mathcal{H}}[\rho(k)\hat{M}(k, b_0, \omega)] \\ &= \text{Tr}_{\mathcal{H}}[\rho(k)M(k, \omega)] = \mu(k, \omega), \end{aligned}$$

$$(19) \quad \begin{aligned} \hat{\mu}'(k, k, b_0, \omega') &= \text{Tr}_{\mathcal{H}'}[\rho'(k)\hat{M}'(k, b_0, \omega')] \\ &= \text{Tr}_{\mathcal{H}'}[\rho(k)M'(k, \omega')] = \mu'(k, \omega'). \end{aligned}$$

For another setting b_1 of \mathbf{B} , however, the expanded explanations can be chosen to conflict in the results they imply. In particular, we are free to choose an explanation in which, independent of k , $\hat{M}(k, b_1)$ is the optimal POVM for deciding between $\rho(k_1)$ and $\rho(k_2)$, while, also independent of k , we take $\hat{M}'(k, b_1)$ to be the optimal POVM for deciding between $\rho'(k_1)$ and $\rho'(k_2)$. The trace functor generates the corresponding probability measures on the extended knob domain:

$$(20) \quad \hat{\mu}(k_j, k, b_1, \omega) = \text{Tr}_{\mathcal{H}}[\rho(k_j)\hat{M}(k, b_1, \omega)],$$

$$(21) \quad \hat{\mu}'(k_j, k, b_1, \omega') = \text{Tr}_{\mathcal{H}'}[\rho'(k_j)\hat{M}'(k, b_1, \omega')],$$

where $j \in \{1, 2\}$. Subtracting the case $j = 2$ from the case $j = 1$ yields

$$(22) \quad \begin{aligned} |\hat{\mu}(k_1, k, b_1, \omega) - \hat{\mu}(k_2, k, b_1, \omega)| &= \left| \text{Tr}_{\mathcal{H}}[\hat{M}(k, b_1, \omega)\{\rho(k_1) - \rho(k_2)\}] \right| \\ &= \frac{1}{2} \text{Tr}_{\mathcal{H}}|\rho(k_1) - \rho(k_2)|, \end{aligned}$$

where the last equality follows from a property of optimal decision operators [10]. For the “primed” extended explanation the same logic implies

$$(23) \quad \begin{aligned} |\hat{\mu}'(k_1, k, b_1, \omega') - \hat{\mu}'(k_2, k, b_1, \omega')| &= \frac{1}{2} \text{Tr}_{\mathcal{H}'}|\rho'(k_1) - \rho'(k_2)| \\ &\neq \frac{1}{2} \text{Tr}_{\mathcal{H}}|\rho(k_1) - \rho(k_2)|, \end{aligned}$$

whence the extensions of the metrically inequivalent explanations $(\mathcal{H}, \rho, M), (\mathcal{H}', \rho', M') \in \text{Tr}^{-1}(\mu)$, for which $\text{MetDev}(\rho, \rho') \neq 0$, though they agree in their implied results on \mathbf{K} , have extensions that imply metrically inequivalent statements of results $\hat{\mu}$ and $\hat{\mu}'$ on $\mathbf{K} \vee \mathbf{L}$ and so conflict in their predictions of knob physics.

The upshot is an open cycle. Expanding the knob domain allows extensions of metrically inequivalent explanations to imply conflicting extended statements of results $\hat{\mu}$ and $\hat{\mu}'$. On rejecting one of these statements, say on the basis of experiment, and assuming the other statement of results, one treats $\hat{\mathbf{K}}$ as a new “given knob domain \mathbf{K} ,” and the cycle starts over, but cycling round investigations of ever-expanding knob domains.

A lesson on the negative side is this. If quantum descriptions are inherently multiple, look for trouble in endeavors that assume the conceptual possibility of a single explanation. For example, many investigators of quantum key distribution [11] have failed to disentangle quantum decision theory from a self-contradictory (usually unspoken) assumption that a single explanation makes sense. Although

quantum key distribution avoids many of the vulnerabilities of classical key transmission, some new potential vulnerabilities arise, at root because of the multiplicity of explanations with their conflicting extensions to a larger knob domain. The conflicting extensions mean that no single explanation can logically substitute for an experimental investigation of that larger domain. For a sketch of the details see Appendix D. On the positive side, acceptance of descriptions as inherently multiple resolves a conceptual muddle, to which we now turn.

6. Making sense of invariance

To demonstrate an invariance we might place a round drinking glass on a table and rotate it to show that “nothing changes under rotation.” But to see this invariance, whether one is aware of it or not, one must manage incompatible frames of reference [12]. Looked at one way “nothing happens when we rotate the glass”; but to see that “nothing happens when we rotate the glass” one must see in the other frame, so to speak, that in fact “the glass rotates,” as evidenced perhaps by a visible speck of dust on the glass or other irregularity that, strictly speaking, violates its symmetry and thereby makes visible its rotation.

Formally, an invariance shows up in a statement of results $\mu: \mathbf{K} \rightarrow \text{PrMeas}(\tilde{\Omega})$ as an equivalence relation E_μ on \mathbf{K} , with equivalence classes

$$E_\mu(k) \stackrel{\text{def}}{=} \{k' | \mu(k', -) = \mu(k, -)\}.$$

Changing k within an equivalence class—a level set—leaves all the probabilities of detections invariant. A colleague at an earlier talk asked “then why not ‘mod out’ the equivalence classes?” Indeed, if certain changes of knob settings make no difference, what experimental evidence do we have to speak of ‘changing a knob setting’ at all?

Yet physicists need to speak of changes that “don’t do anything.” For example, special relativity deals with how nothing changes when a train is put in uniform motion relative to a station. But, just as in the water glass, the “nothing changes” must be seen also from a conflicting viewpoint in which “the train moves.” If one tries to condense the concept of invariance into a single description, one meets confusion; while if we recognize that multiplicity of description as part and parcel of the concept of description, two levels of description suffice to make invariance comprehensible.

Here is an example involving mapping a detector domain $\tilde{\Omega}$ into a larger detector domain $\tilde{\Omega}' = \tilde{\Omega} \vee \tilde{\Omega}''$, where $\tilde{\Omega} \wedge \tilde{\Omega}'' = \emptyset$; in effect $\tilde{\Omega}'$ augments $\tilde{\Omega}$ with an additional detector. The mapping is the injection $g: \tilde{\Omega} \hookrightarrow \tilde{\Omega}'$ that assigns to each (ω) in the smaller detector domain $\tilde{\Omega}$ the element $(\omega, \Omega'') \in \tilde{\Omega}'$. (In effect, $g(\omega)$ ignores the detectors of $\tilde{\Omega}'$ other than those expressed by $\tilde{\Omega}$.) The injection g induces a “contravariant” map $F_g: \text{PPM}(\mathbf{K}, \tilde{\Omega}') \rightarrow \text{PPM}(\mathbf{K}, \tilde{\Omega})$ that corresponds to marginal probability; that is F_g is defined by

$$(24) \quad F_g(\mu') = \mu \text{ s.t. } (\forall k \in \mathbf{K}, \omega \in \tilde{\Omega}) \quad \mu(k, \omega) = \mu'(k, g(\omega)) = \mu'(k, (\omega, \Omega'')).$$

The extra detail needed to “see the glass move” shows up in the finer-level statement of results μ' , with its dependence on an extra detector that, like the speck of dust, expresses what happened that left the marginal probabilities μ invariant. Taking the marginal parametrized probability obtained by ignoring the extra detector, we get $\mu'[k, (\omega, \Omega'')] = \mu(k, \omega)$, so the invariance in μ is retrieved,

now seen as a *marginal* parametrized probability measure, derived from a more complex parametrized probability measure μ' .

7. Discussion

In broad terms, we offer here a recognition of guesswork as a third pillar of science along side of calculation and measurement. Among the giants on whose shoulders we stand are Ernst Mach and those of his intellectual descendants, Heisenberg among them, who worried that theory seemed so remote from life in a laboratory equipped with instruments of measurement. We owe a debt to both the push toward operationalism and the counter-push that recognizes the need for theoretical constructs having no direct counterparts on the lab bench. Tracing out the history of these ideas in relation to an acceptance of ambiguity and the consequent role of guesswork is an appealing project for a future collaboration with the historically literate.

We introduce the unfamiliar term *explanation* for the vectors and operators of a quantum description to contrast them with the probabilities which we say are explained. This contrast is plain enough to see in the texts of Dirac and von Neumann, etc. but we aimed to highlight it. Striking to us is the way quantum theory provides both structure and ambiguity, and the structure of probabilities becomes an essential ingredient in ambiguity of outcomes, as here conceived.

We were asked about the relationship of our work to elements of quantum logic and quantum probability theory. Quantum logic expresses measurement outcomes as subspaces of a Hilbert space, while we express measurement outcomes as a field of sets, in the sense of Kolmogorov [13], without any reference to a Hilbert space. By detaching our concept of an event from a Hilbert space, we acquire the power to speak of differing explanations involving differing Hilbert spaces that “explain” the same probabilities of outcomes. Within any single explanation, the outcomes explained can be made to correspond to subspaces of a Hilbert space (perhaps with the use of Neumark’s theorem [14] to convert an arbitrary POVM to a projective POVM).

In connection with quantum logic, we were asked about the relation of our work to that of Birkhoff and von Neumann [15], who showed a role for two distinct lattices, one to do with their propositional calculus, the other to do with subspaces of a Hilbert space. We are on the side of those who notice that in their demonstrations of lattice properties, Birkhoff and von Neumann use garden-variety propositional logic, and not their quantum logic, which to us is an interesting display of lattice structures. Naming the lattice structure of Hilbert spaces “quantum logic” seems to us a misnomer that confuses the unwary. As amateurs looking from “outside,” we enjoy the disparate views among mathematicians and logicians about suitable rules for the game of logic; we have not yet seen anything that can reasonably be termed “quantum” about logic.

We were asked also about the relation of our work to Gleason’s theorem. The short answer is that we notice that in physics the Hilbert space is never an experimental fact, but requires an act of guesswork. Once one guesses a Hilbert space, then certainly Gleason’s theorem comes into play, and our work is consistent with it, because we pay attention to knob domains that are roughly speaking smaller than the space of operators on a Hilbert space. By way of justification for the focus on knob domains that are “small” relative to a space of operators, note that choosing

an explanation involving a Hilbert space to which Gleason's theorem pertains, and taking the knob domain to be the whole space of density operators and POVMs on that Hilbert space, there is always an alternative explanation involving a larger Hilbert space with its larger space of operators, relative to which that knob domain becomes "small."

Acknowledgments

We are grateful for the invitation to present a preliminary version of this paper at the Conference on Representation Theory, Quantum Field Theory, Category Theory, Mathematical Physics and Quantum Information Theory, funded by the National Science Foundation, September 20–23, 2007, at The University of Texas at Tyler, organized by Kazem Mahdavi, Louis Kauffman, Samuel Lomonaco, and Deborah Koslover. We also thank Sam Lomonaco for helpful suggestions. We thank an anonymous referee for posing the questions to which we respond in the Discussion section.

Appendix A. Unordered products of knobs and detectors

For any set X of sets, the unordered product πX is a set of pairs, with each pair of the form (a, A) , where $a \in A$, with exactly one pair for each set in X . E.g., if $X = \{A, B, C\}$, then $\pi X = \{ \{(a, A), (b, B), (c, C)\} \mid a \in A, b \in B, c \in C \}$. We call the sets $A, B, C \in X$ *factors* of the unordered product πX . Unordered products of sets constitute a lattice with a partial order, join, meet and difference defined by

$$(25) \quad \pi X \leq \pi Y \stackrel{\text{def}}{=} X \subset Y,$$

$$(26) \quad \pi X \vee \pi Y \stackrel{\text{def}}{=} \pi(X \cup Y),$$

$$(27) \quad \pi X \wedge \pi Y \stackrel{\text{def}}{=} \pi(X \cap Y),$$

$$(28) \quad \pi X - \pi Y \stackrel{\text{def}}{=} \pi(X - Y),$$

where $X - Y$ is the set difference: $X - Y \stackrel{\text{def}}{=} \{a \mid a \in X \text{ and } a \notin Y\}$.

Definition: Understanding a *knob* to be a set of knob settings, a *knob domain* is an unordered product of knobs. We call an element of a knob domain a setting (of that domain); it conveys the settings of all the knobs of the domain.

Remarks:

- (1) A knob domain resembles a cartesian product of knobs, except that: (a) it excludes the possibility of the same knob appearing twice; and (b) it avoids the ordering presumed by a cartesian product. Both of these exceptions to the cartesian product are required for a *join* of two knob domains, defined below, to make sense.
- (2) Underlying any knob domain \mathbf{K} is its set of knobs which we denote by $\pi^{-1}\mathbf{K}$. This π^{-1} is a forgetful functor from unordered products to their underlying sets. It follows that

$$(29) \quad (\text{for } X \text{ any set of sets}) \quad \pi^{-1}(\pi X) = X,$$

and

$$(30) \quad (\text{for } \mathbf{K} \text{ any knob domain}) \quad \pi(\pi^{-1}\mathbf{K}) = \mathbf{K}.$$

Their definition as unordered products implies that a set of knob domains has a lattice structure, handy for expressing the relation between two experiments that share some but not all of the same knobs. Given two knob domains \mathbf{K} and \mathbf{K}' , their meet $\mathbf{K} \wedge \mathbf{K}'$ amounts to the knobs they share in common, while their join is related to the join of their underlying unordered products.

By way of the forgetful functor π^{-1} that takes an unordered product to the set of its underlying sets, this lattice of knob domains is defined, for any two knob domains \mathbf{K} and \mathbf{K}' , by the following:

$$(31) \quad \mathbf{K} \leq \mathbf{K}' \stackrel{\text{def}}{=} \pi^{-1}(\mathbf{K}) \subset \pi^{-1}(\mathbf{K}'),$$

$$(32) \quad \mathbf{K} \vee \mathbf{K}' \stackrel{\text{def}}{=} \pi[\pi^{-1}(\mathbf{K}) \cup \pi^{-1}(\mathbf{K}')],$$

$$(33) \quad \mathbf{K} \wedge \mathbf{K}' \stackrel{\text{def}}{=} \pi[\pi^{-1}(\mathbf{K}) \cap \pi^{-1}(\mathbf{K}')],$$

$$(34) \quad \mathbf{K}' - \mathbf{K} \stackrel{\text{def}}{=} \pi[\pi^{-1}(\mathbf{K}') - \pi^{-1}(\mathbf{K})].$$

If two knob domains share no common knob in their underlying sets, we have $\mathbf{K} \wedge \mathbf{K}' = \emptyset$. In case $\mathbf{K} \wedge \mathbf{K}' = \emptyset$ (and only in this case), an isomorphism takes any (x, y) with $x \in \mathbf{K}$ and $y \in \mathbf{K}'$ to an element $z \in \mathbf{K} \vee \mathbf{K}'$. We express this isomorphism as

$$(35) \quad z = x \vee y.$$

Two distinct ways of getting less than a knob domain play a role. Given a knob domain \mathbf{K}' , we can be interested in a domain \mathbf{K} that has some but not all of the same knobs, a relation written as $\mathbf{K} < \mathbf{K}'$. Or, we can be interested in a subset of $\mathbf{L} \subsetneq \mathbf{K}'$. Each element of \mathbf{L} specifies a setting of each knob of \mathbf{K}' but some of the elements of \mathbf{K}' are absent from \mathbf{L} .

Correspondingly, two levels of set differences enter the story. If $\mathbf{L} \subset \mathbf{K}$, then $\mathbf{K} - \mathbf{L} \stackrel{\text{def}}{=} \{x | x \in \mathbf{K} \text{ and } x \notin \mathbf{L}\}$. This is the ordinary set difference. We also want another kind of difference that applies to two knob domains \mathbf{K} and \mathbf{K}' . If the two knob domains do not share all the same knobs, they have no elements in common (so that $\mathbf{K}' - \mathbf{K} = \mathbf{K}'$); we use $\overset{\pi}{-}$ in the expression $\mathbf{K}' \overset{\pi}{-} \mathbf{K}$ to indicate the knob domain is an unordered product of those factors of \mathbf{K}' that are not factors of \mathbf{K} .

A.1. Detector domains. We suppose that each detector separately is expressed mathematically by an outcome space. To each outcome space Ω there is associated a set $\tilde{\Omega}$ of the measurable subsets of Ω . Now extend this construction by letting $\mathbf{\Omega}$ be the unordered product of a set of outcome spaces $\{\Omega_A, \Omega_B, \dots\}$. Let $\tilde{\mathbf{\Omega}}$ be the set of measurable subsets of this product, constructed in analogy with the construction for cartesian products of measure spaces, and call such an entity a *detector domain*. A detector domain $\tilde{\mathbf{\Omega}}$ built up from more than one outcome set contains, in addition to unordered measurable rectangles, unions of disjoint measurable rectangles; indeed it is defined to be a σ -algebra [16].

In parallel with the story for knobs, for detectors we have a lattice of unordered products of outcome spaces. This lattice of unordered products of outcome spaces induces a lattice of detector domains defined by

$$(36) \quad \tilde{\Omega} \leq \tilde{\Omega}' \stackrel{\text{def}}{=} \Omega \leq \Omega',$$

$$(37) \quad \tilde{\Omega} \vee \tilde{\Omega}' \stackrel{\text{def}}{=} \widetilde{\Omega \vee \Omega'},$$

$$(38) \quad \tilde{\Omega} \wedge \tilde{\Omega}' \stackrel{\text{def}}{=} \widetilde{\Omega \wedge \Omega'},$$

$$(39) \quad \tilde{\Omega}' \overset{\pi}{-} \tilde{\Omega} \stackrel{\text{def}}{=} \widetilde{\Omega' \overset{\pi}{-} \Omega}.$$

Appendix B. Metric deviation of two functions having the same domain but possibly distinct codomains

Consider any two spaces Y and Y' equipped with bounded metrics d and d' , respectively; let X be any set of more than one element. We define the *metric deviation* between any two functions $f : X \rightarrow Y$ and $f' : X \rightarrow Y'$ by

$$(40) \quad \text{MetDev}(f, f') \stackrel{\text{def}}{=} \sup_{x_1, x_2 \in X} |d(f(x_1), f(x_2)) - d'(f'(x_1), f'(x_2))|.$$

If the deviation is zero, we speak of f and f' as *metrically equivalent*.

In the case $Y = Y'$, the functions f and f' can also be compared by the uniform metric. In this case the metric deviation is a coarser comparison than the uniform

metric, and it is this coarser comparison that is most relevant to what detections can tell about the structure of knob domains.

B.1. Topology induced on a domain by a function to a space. Let Y be any topological space with topology τ_Y , let X be any set, and let f be any function from the domain X to Y . Then f partitions X into equivalence classes by the relation

$$(41) \quad xE_f x' \Leftrightarrow f(x) = f(x').$$

Let X/E_f be the quotient set (set of equivalence classes) of X by E_f , and define the projection

$$(42) \quad p_f: X \rightarrow X/E_f.$$

(1) Define a topology τ_f on the domain X by

$$(43) \quad \tau_f = \{U | (\exists V \in \tau_Y) \quad U = f^{-1}(V)\}.$$

(2) Consider X/E_f with the topology $p_f \tau_f \stackrel{\text{def}}{=} \{W | (\exists U \in \tau_f) \quad W = p_f U\}$. X/E_f with this topology is homeomorphic to $\text{Im } f$ with its subspace topology inherited from τ_Y .

(3) Any metric d on Y induces a metric d_f on X/E_f :

$$(44) \quad d_f(p_f x_1, p_f x_2) \stackrel{\text{def}}{=} d[f(x_1), f(x_2)].$$

(4) If Y has a metric d and f is injective, then d_f is a metric on X .

Lemma: For $f: X \rightarrow Y$ and $f': X \rightarrow Y$, if $\text{MetDev}(f, f') = 0$ then

$$(45) \quad \tau_f = \tau_{f'} \text{ and } d_f = d_{f'}.$$

Proof: $\text{MetDev}(f, f') = 0 \Rightarrow E_f = E_{f'}$, whence follows $\tau_f = \tau_{f'}$. \square

Appendix C. Diverse explanations of given results

Although statements of results leave open choices of explanations, they do indeed impose some constraints. Here we show that except in limiting special cases these constraints leave metrically inequivalent density-operator functions available for explanations within $\text{Tr}^{-1}(\mu)$.

In [4] we rather arbitrarily imposed an additional constraint on explanations (which in that paper we called *models*) by separating control over the density operator from control over the POVM, so that a knob domain has the form $\mathbf{K} = \mathbf{A} \times \mathbf{B}$, with

$$(46) \quad (\forall k \in \mathbf{K})(\exists a \in \mathbf{A}, b \in \mathbf{B}) \quad k = (a, b).$$

From Propositions 2 and 4 of [4] follows the

Proposition: Even under this additional constraint on explanations, there are metrically inequivalent density operators in $\text{Tr}^{-1}(\mu)$ *unless*

$$(47) \quad (\forall a_1, a_2 \in \mathbf{A})(\exists b \in \mathbf{B}) \quad D_{\mathbf{N}}[\mu(a_1, b), \mu(a_2, b)] = 1.$$

C.1. Constraint on explanations imposed by given results. A simpler if weaker demonstration of constraints imposed by results than that given in [4] is the following. A given statement of results $\mu \in \text{PPM}(\mathbf{K}, \tilde{\Omega})$ imposes some constraints on explanations, as follows. Using the definition of D_{Ω} given in Eq. (4),

$$\begin{aligned}
 (\forall(\mathcal{H}, \rho, M) \in \text{Tr}^{-1}(\mu)) \quad & D_{\Omega}[\mu(k_1, -), \mu(k_2, -)] \\
 = \quad & \sup_{\omega \in \tilde{\Omega}} \text{Tr}_{\mathcal{H}}[\rho(k_1)M(k_1, \omega) - \rho(k_2)M(k_2, \omega)] \\
 = \quad & \sup_{\omega \in \tilde{\Omega}} (\text{Tr}_{\mathcal{H}}\{\rho(k_1) - \rho(k_2)\}M(k_1, \omega) + \text{Tr}_{\mathcal{H}}\{\rho(k_2)[M(k_1, \omega) - M(k_2, \omega)]\}) \\
 \leq \quad & \sup_{M' \in \text{DetectOp}(\mathcal{H})} \text{Tr}\{M'[\rho(k_1) - \rho(k_2)]\} \\
 & + \sup_{\rho' \in \text{DensOp}(\mathcal{H})} \text{Tr}_{\mathcal{H}}\{\rho'[M(k_1, \omega) - M(k_2, \omega)]\} \\
 (48) = \quad & \frac{1}{2} \text{Tr}_{\mathcal{H}}|\rho(k_1) - \rho(k_2)| + \sup_{\omega \in \tilde{\Omega}} \|M(k_1, \omega) - M(k_2, \omega)\|_{\mathcal{H}}.
 \end{aligned}$$

The last equality makes use of the relation shown in [10] for trace distance and also hermitian property of detection operators.

Appendix D. Ambiguity of explanations in quantum cryptography

In quantum cryptography, specifically quantum key distribution, untenable claims of absolute security against undetected eavesdropping have arisen from the tacit supposition of a single explanation of experimental results. Under that supposition, security claims invoke a theorem of quantum decision theory that tells how the minimum probability of error for deciding between two states $\rho(1)$ and $\rho(2)$ rises as their trace distance decreases. For example, without regard to the multiplicity of explanations available for any given probabilities, the popular design BB84 [17] invokes a single explanation in which pairs of states $\rho(1)$ and $\rho(2)$ exhibit a trace distance less than or equal to $2^{-1/2}$, implying a minimum probability of error to decide between them:

$$(49) \quad P_E \geq \frac{1}{2}(1 - \frac{1}{2}|\rho(1) - \rho(2)|) = \frac{1}{2}(1 - \sqrt{\frac{1}{2}}) \approx 0.146.$$

But how is one to rely on an implemented key-distribution system built from lasers and optical fibers and so forth to act in accordance with this explanation? If a system of lasers and optical fibers and so forth “possessed” a single explanation in terms of quantum states, one could hope to test experimentally the trace distance between the pair of states. But no such luck. The trouble is that trace distance is a property not of probabilities *per se*, which are testable, but of some one among the many *explanations* of those probabilities. While the testable probabilities constrain the possible explanations, and hence constrain trace distances, this constraint on trace distance is “the wrong way around”—a lower bound instead of a sub-unity upper bound on which security claims depend.

Given any parametrized probability measure, proposition 2 in [4] assures the existence of an explanation in terms of a parametrized density operator ρ' metrically inequivalent to ρ , such that, in conflict with Eq. (49), the trace distance becomes $\frac{1}{2}|\rho'(1) - \rho'(2)| = 1$, making the quantum states in this explanation distinguishable without error, so that the keys that they carry are totally insecure.

The central issue in key distribution is this: how will the lasers and fibers and detectors that convey the key respond to attacks, in which an as yet unknown eavesdropper brings extra devices with their own knobs and detectors into contact with the key-distributing system? Attacks entail knob and/or detector domains extended beyond those tested, with the possibility that extended explanations metrically inequivalent to that used in the design, but consistent with available probabilities, both imply a lack of security theoretically and accord with actual eavesdropping.

Physically, one way for insecurity to arise is by an information leak through frequency side-band undescribed in the explanation on which system designers relied. A more likely security hole appears when lasers that are intended to radiate at the same light frequency actually radiate at slightly different frequencies, as described in [5, 18, 19].

References

- [1] Louis H. Kauffman, "Time imaginary value, paradox sign and space," in *Computing Anticipatory Systems*, CASYS – Fifth International Conference, Liege, Belgium (2001), Daniel Dubois, ed., AIP Conference Proceedings Volume 627, 2002.
- [2] J. M. Myers and F. H. Madjid, "A proof that measured data and equations of quantum mechanics can be linked only by guesswork," *Quantum Computation and Information*, S. J. Lomonaco, Jr. and H. E. Brandt, eds., Contemporary Mathematics Series, Vol. 305, pp. 221–244, American Mathematical Society, Providence, RI, 2002.
- [3] J. M. Myers and F. H. Madjid, "Gaps between equations and experiments in quantum cryptography," *J. Opt. B: Quantum Semiclass. Opt.* **4**, pp. S109–S116, 2002.
- [4] F. H. Madjid and J. M. Myers, "Matched detectors as definers of force," *Annals of Physics (NY)* **319**, pp. 251–273, 2005.
- [5] J. M. Myers and F. H. Madjid, "What probabilities tell about quantum systems, with application to entropy and entanglement," in *Philosophy of Quantum Information and Entanglement*, A. Bokulich and G. Jaeger, eds., Cambridge University Press, *in press*.
- [6] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 4th ed., Clarendon Press, Oxford, 1958.
- [7] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer, Berlin, 1932; translated with revisions by the author as *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, NJ, 1955.
- [8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
- [9] W. Rudin, *Functional Analysis*, 2nd ed., McGraw-Hill, New York, 1991.
- [10] M. A. Nielsen and I. L. Chuang, *op. cit.*, p. 404.
- [11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, pp. 145–195, 2002.
- [12] W. Byers, *How Mathematicians Think: Using Ambiguity, Contradiction, and Paradox to Create Mathematics*, Princeton University Press, Princeton, NJ, 2007.
- [13] A. N. Kolmogorov, *Foundations of the Theory of Probability*, 2nd English ed., Chelsea Publishing Company, New York, 1956.
- [14] J. M. Myers, "Conditional probabilities and density operators in quantum modeling," *Foundations of Physics* **36**, pp. 1012–1035, 2006.
- [15] G. Birkhoff and J. von Neumann, "The logic of quantum mechanics," *Annals of Mathematics* **37**, pp. 823–843, 1936.
- [16] W. Rudin, *Real and Complex Analysis*, 3rd ed., McGraw-Hill, New York, 1987.
- [17] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key-distribution and coin tossing," *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India*, pp. 175–179, IEEE, New York, 1984.
- [18] J. M. Myers, "Polarization-entangled light for quantum key distribution: how frequency spectrum and energy affect statistics," *Proceedings of SPIE*, Vol. 5815, Quantum Information and Computation III, E. J. Donkor, A. R. Pirich, H. E. Brandt, eds., pp. 13–26, SPIE, Bellingham, WA, 2005.
- [19] J. M. Myers "Framework for quantum modeling of fiber-optical networks, Parts I and II," arXiv:quant-ph/0411107v2 and quant-ph/0411108v2, 2005.

SCHOOL OF ENGINEERING AND APPLIED SCIENCES, HARVARD UNIVERSITY, 60 OXFORD STREET, CAMBRIDGE, MA 02138

E-mail address: myers@seas.harvard.edu

82 POWERS ROAD, CONCORD, MA 01742

E-mail address: gmadjid@aol.com

This page intentionally left blank

Reference Frame Fields based on Quantum Theory Representations of Real and Complex Numbers

Paul Benioff

ABSTRACT. A quantum theory representations of real (R) and complex (C) numbers is given that is based on states of single, finite strings of qukits for any base $k \geq 2$. Arithmetic and transformation properties of these states are given, both for basis states representing rational numbers and linear superpositions of these states. Both unary representations and the possibility that qukits with k a prime number are elementary and the rest composite are discussed. Cauchy sequences of q_k string states are defined from the arithmetic properties. The representations of R and C , as equivalence classes of these sequences, differ from classical representations as kit string states in two ways: the freedom of choice of basis states, and the fact that each quantum theory representation is part of a mathematical structure that is itself based on the real and complex numbers. In particular, states of qukit strings are elements of Hilbert spaces, which are vector spaces over the complex field. These aspects enable the description of 3 dimensional frame fields labeled by different k values, different basis or gauge choices, and different iteration stages. The reference frames in the field are based on each R and C representation where each frame contains representations of all physical theories as mathematical structures based on the R and C representation. Some approaches to integrating this work with physics are described. It is observed that R and C values of physical quantities, matrix elements, etc. which are viewed in a frame as elementary and featureless, are seen in a parent frame as equivalence classes of Cauchy sequences of states of qukit strings.

1. Introduction

Numbers play a basic role in physics and mathematics, so basic in fact that their use, both in experiments and in theory, is taken for granted and is rarely examined. Natural numbers and integers are probably the most basic because of their role in counting, rational numbers play a basic role in that numerical experimental outputs are represented as rational numbers. They also are the type of numbers used in all computer computations.

The importance of real and complex numbers lies in their being the number base of all physical theories used so far. This includes classical and quantum

1991 *Mathematics Subject Classification.* 81V99,81Q99.

Key words and phrases. Quantum Numbers, Qukit Strings, Frame Fields.

mechanics, quantum field theory, QED, QCD, string theory, and special and general relativity. Each of these theories is a mathematical theory characterized by a different set of axioms. Assuming the axiom sets are consistent, each theory has many different representations as mathematical structures based on the real and complex numbers. The connection to physics is made by interpreting some of the elements in the mathematical structures as representing physical systems and physical quantities. Examples include the use, in quantum theory, of elements of Hilbert spaces and operators on the spaces to represent states and observable physical quantities of systems, the use of other elements, to represent various properties of space time, etc.

In all of this, the tacit assumption is made that the properties of physical systems and the physical universe are independent of the properties of mathematical theories and their representations. The general approach taken is to discover the theory that best describes physical systems and their properties. Little attention is paid to whether the basic properties of theories and their mathematical representations have any influence on the basic properties of physical systems or how intertwined physics and mathematics are.

The approach taken in this paper stems from the work of Wigner on the unreasonable effectiveness of mathematics in the natural sciences [1, 2, 3]. One answer to this problem is that one should work towards developing a coherent theory of mathematics and physics together [4, 5]. Presumably such a theory would show why mathematics is important to physics.

This paper is, hopefully, a step in this direction. Here extension of previous work on the quantum representation of numbers [6, 7] shows that quantum theory representations of real and complex numbers have properties not possessed by classical representations of these numbers. It will be seen that the structures resulting from these properties suggest a close intertwining between the properties of physical and mathematical systems.

Although little investigated, these possibilities are not new. Perhaps the closest is the work of Tegmark [8, 9] which suggests that the physical universe really is a mathematical structure. Other work which emphasizes the close relationship between physics and mathematics is concerned with quantum theory representations of mathematical systems. This work includes papers on quantum set theory [10, 11, 12], quantum theory representations of real numbers [13, 14, 15, 16, 17, 18, 19], and the use of category theory in physics [20, 21].

The quantum representations of real and complex numbers presented here differ from other work in this area in that they are not abstract representations based on quantum logic or on lattice valued models of set theory [13, 14, 15, 17, 18], nonstandard numbers [16], or category theory [20, 21]. Instead they are based on representations of natural numbers, N , integers, I , and rational numbers, Ra , as states of finite strings of qukits.¹

This choice is based on the observation that all physical representations of numbers are in the form of k -ary representations as states of strings of kits or of qukits. This is the case for all experimental outputs. Also all computations are

¹Qukits are extensions of qubits to systems with states in a finite k dimensional Hilbert space.

based on these representations of numbers. The importance of this type of number for computations and the limits of computation suggest other ties to information theory and limitations on the information resources of the universe [22, 23, 24]. The restriction here to qubit strings is based on the fact that quantum theory is the basic underlying theory of all physical systems.

Here the quantum theory representations of real numbers are described as equivalence classes of Cauchy sequences of states of qubit strings. In essence this is a translation of the definition in mathematical analysis textbooks [25, 26] as equivalence classes of Cauchy sequences of rational numbers into quantum theory.²

These representations are described in the next two sections. First quantum representations of natural numbers, integers, and rational numbers are presented as states of single finite qubit strings. These are based on the states of each qubit as elements of a k dimensional Hilbert space. These are used in the quantum representations of real numbers as equivalence classes of Cauchy sequences of states of single finite qubit strings.

Quantum representations of real and complex numbers differ from classical representations in several ways. One difference is that the equivalence classes of Cauchy sequences of qubit string states are larger than classical classes as they contain sequences that do not correspond to any classical sequence. However, no new equivalence classes are created.

A more important difference is that, for states of qubit strings, there is a freedom of basis state choice that does not exist in classical representations. This is based on the observation that the states of each qubit are elements of a k dimensional Hilbert space. In order that states of qubits, (q_k) , represent numbers, one must choose a basis set of states for each q_k in the string. This is well known in quantum computation where binary representations of numbers, such as $|1100101\rangle$ as a state of a qubit string, imply a choice of basis for each qubit. This freedom of basis choice is also referred to here as a gauge freedom or freedom to fix a gauge for each q_k . It is represented here by a variable g that ranges over all basis or gauge choices for q_k states in a string. This gauge freedom is seen to extend up to representations of real numbers in that for each gauge choice g one has quantum theory representations $R_{k,g}$ of real numbers that are different for different k and g . Even though these representations are k, g dependent, they are all isomorphic to one another.

These representations for different k and g are described in section 4. Both base changing transformations and gauge transformations are described for the finite q_k string states. Lifting these up to transformations on the Cauchy sequences gives transformations that take one real number representation to another, $R_{k,g} \rightarrow R_{k',g'}$.

The description is extended to include quantum theory representations of complex numbers, $C_{k,g}$, in section 5. They are defined as equivalence classes of Cauchy sequences of states of pairs of finite q_k strings where the pair elements correspond to real and imaginary parts of a complex rational number. Cauchy

²An often used equivalent definition is based on Dedekind cuts of rational numbers instead of Cauchy sequences.

conditions are applied separately to the sequences of real and imaginary components.

There is another very important difference between quantum and classical representations of real and complex numbers. This is the fact that the states of the q_k strings used to define Cauchy sequences are elements of a Fock space that is itself a vector space over a field of real and complex numbers. For example all eigenvalues of operators acting on these string states are complex or real numbers. Also all linear superposition coefficients are complex numbers. This is quite different from the classical situation in that real and complex numbers play no role in the representation of numbers as states of bit or kit strings.

This dependence of quantum theory representations on the real and complex number base of spaces of q_k string states leads to the possibility of iteration of the construction. Each representation $R_{k,g}, C_{k,g}$ can serve as the real and complex number base of Hilbert space and Fock space representations of q_k string states that can be used to construct other representations of the real and complex numbers.

In addition, this same iteration possibility extends to all physical theories that are representable as mathematical structures over the real and complex numbers. Included are quantum and classical mechanics, quantum field theory, special and general relativity, string theory, as well as other theories.

This leads to the association of a reference frame $F_{k,g}$ to each representation $R_{k,g}, C_{k,g}$. Each frame $F_{k,g}$ contains representations of all physical theories as mathematical structures based on $R_{k,g}, C_{k,g}$. This use of reference frame terminology is consistent with other uses [27, 28] in that it sets a base or reference point $R_{k,U}, C_{k,U}$ for representations of all physical theories.

Much of the rest of the paper, Section 6, is concerned with properties of these reference frames and with three dimensional fields of these reference frames. Two of the dimensions are labeled by k and g . The third is by an integer j denoting the iteration stage. Different iteration possibilities are considered: finite, one way infinite, two way infinite, and cyclic. Also properties of observers in different locations in the frame field are described.

Section 7 includes a discussion on what is probably the most important outstanding issue, how to integrate the frame field with physics. This is especially important from the viewpoint of constructing a coherent theory of physics and mathematics together [4, 5] or if one considers the physical universe as a mathematical universe [8, 9]. Both relatively simple aspects of the possible integration, and more speculative aspects are described. However it is clear from this that much remains to be done to achieve an integration with physics.

The discussion section includes a description of the possible replacement of Cauchy sequences by operators, a possible use of gauge theory to integrate this work with physics, and other issues.

Two aspects of the following work should be emphasized. One is that rational numbers are represented by states of *single* qubit strings and not by states of pairs of qubit strings. This is based on the observation that all physical representations of rational numbers, such as computer inputs and outputs, outcomes of measurements, physical constants, etc. are as single strings of digits in some base $k \geq 2$ (usually 2 or 10) and not as integer pairs. Also complex numbers are represented in

computations by pairs of finite digit strings in some base where the pair elements correspond to the real and imaginary components. The use of this representation is based on the fact that sets of rational numbers so represented are dense in the sets of all rational and all real numbers.

In this paper basic arithmetic relations and operations for the different types of numbers are discussed. The reason for this is based on the observation that states of kit or qukit strings, such as $|100101\rangle$ for $k = 2$, do not, in any ab initio sense, represent numbers of any type. In order to show that these states represent numbers, one must prove that they satisfy a relevant set of axioms. The axioms are expressed in terms of properties of basic arithmetic relations and operations. It follows that a proof that sets of states of finite q_k strings represent numbers is based on showing that definitions of these relations and operations satisfy the relevant axiom sets. Some details of these proofs, which are based on classical proofs, [25], are given in [6, 29].

2. Quantum Representations of Natural Numbers, Integers, and Rational Numbers

2.1. Representations. The quantum representations of numbers are described here by states of strings of qukits on a two dimensional integer lattice, $I \times I$. The states are given by $|\gamma, 0, h, s\rangle_{k,g}$ where s is a $0, 1, \dots, k-1$ valued function on an interval $[l, h; u, h]$ of $I \times I$, with $l \leq 0 \leq u$, $\gamma = +, -$ denotes the sign, and $0, h$ the lattice location of the $k - al$ point. The reason for the subscript g will be clarified later on.

Here it is intended that the states $|\gamma, 0, h, s\rangle_{k,g}$ represent numbers in N, I , and Ra . For numbers in N , $\gamma = +, l = 0$; for numbers in I , $l = 0$, and there are no restrictions for Ra . A compact notation is used where the location of the sign, denoted by $0, h$, is also the location of the $k - al$ point. As examples, the base 10 numbers 612, -0474 , -012.7100 are represented here by $|612+\rangle$, $|0474-\rangle$, $|012 - 7100\rangle$ respectively. Note that leading and trailing 0s are allowed.

The states $|\gamma, 0, h, s\rangle_{k,g}$ can be represented in terms of creation operators acting on the qukit vacuum state $|0\rangle$ where

$$(1) \quad |\gamma, 0, h, s\rangle_k = c_{\gamma,0,h}^\dagger a_{s(u,h),u,h}^\dagger \cdots a_{s(l,h),l,h}^\dagger |0\rangle = c_{\gamma,0,h}^\dagger (a^\dagger)_h^s |0\rangle.$$

Here $c_{\gamma,0,h}^\dagger$ creates a sign qubit at $(0, h)$ and $a_{i,j,h}^\dagger$ creates a qukit in state $i = 0, 1, \dots, k-1$ at (j, h) . $(a^\dagger)_h^s$ is a short representation of the string of a^\dagger operators.

The creation operators and the corresponding annihilation operators satisfy the usual commutation or anticommutation rules for respective boson or fermion qukits. The variable h is present to allow for the presence of $n - tuples$ of q_k string states representing $n - tuples$ of numbers.

The use of $I \times I$ as a framework for qukit state representations is based on the need to distinguish qukits in a string by a discrete ordering parameter and to distinguish different qukit strings from one another. This is seen in Eq. 1 where the integers j with $l \leq j \leq u$ order the qukits in a string and the values of h serve to distinguish different strings. There is no need to consider $I \times I$ as a lattice of

points in a two dimensional physical space as its sole function is to provide discrete ordering and distinguishing labels.

Also the locations of the qukit strings in the lattice direction of the strings will be restricted in that the sign qubit will always be at site 0. This restriction is inessential because the only function of the j label in (j, h) is to provide a discrete ordering of qukits states in a string.

The set of states $|\gamma, 0, h, s\rangle_{k,g}$ for all γ, h, s are a basis, $\mathcal{B}_{k,h,g}$, that spans a Fock space $\mathcal{F}_{k,h}$ of states that are linear superpositions

$$(2) \quad \psi = \sum_{\gamma, h, s} c_{\gamma, h, s} |\gamma, 0, h, s\rangle_{k,g}$$

Here and in the following, $\sum_s = \sum_{l \leq 0} \sum_{u \geq 0} \sum_{s_{[l,u]}}$ is a sum over all integer intervals $[l, u]$ and over all $0, 1, \dots, k-1$ valued functions s with domain $[l, u]$. A Fock space is used because states of q_k strings with different numbers of qukits are included. The subscript $k \geq 2$ denotes the base. Note that base k qukits are different from base k' qukits just as spin k systems are different from spin k' systems.

Extension of the description to include pairs, triples and n -tuples of basis states and their linear superpositions is done by distinguishing different states in the tuples with different values of h . For each finite subset $S = h_1, h_2, \dots, h_{|S|}$ of integers where $|S|$ is the number of integers in S , let $\mathcal{B}_{k,S,g}$ be the set of states of the form $|\gamma_1, 0, h_1 s_1\rangle_k |\gamma_2, 0, h_2 s_2\rangle_k \cdots |\gamma_{|S|}, 0, h_{|S|} s_{|S|}\rangle_k$. Define $\mathcal{B}_{k,g}$ by

$$(3) \quad \mathcal{B}_{k,g} = \bigcup_S \mathcal{B}_{k,S,g}.$$

$\mathcal{B}_{k,g}$ is a basis set of all finite tuples of states of finite q_k strings. Let \mathcal{F}_k be the Fock space spanned by the states in $\mathcal{B}_{k,g}$.

The representation of state n -tuples used here is by products of states as in $|\gamma_1, 0, h_1, s_1\rangle_{k,g} \cdots |\gamma_{|S|}, 0, h_{|S|}, s_{|S|}\rangle_{k,g}$. The A-C operator representation of this state is $c_{\gamma_1, 0, h_1}^\dagger (a^\dagger)_{h_1}^{s_1} \cdots c_{\gamma_{|S|}, 0, h_{|S|}}^\dagger (a^\dagger)_{h_{|S|}}^{s_{|S|}} |0\rangle$. For bosons the ordering of the operators is immaterial. For fermions a specific ordering must be selected as a canonical ordering.

The basic arithmetic relations needed to show that the states $|\gamma, 0, h, s\rangle_{k,g}$ do represent numbers are equality $=_{A,k,g}$ and less than $<_{A,k,g}$.³

$$(4) \quad |\gamma, 0, h, s\rangle_{k,g} =_{A,k,g} |\gamma', 0, h', s'\rangle_{k,g}$$

holds if $\gamma' = \gamma$ and $s' = s$ up to leading and trailing 0s.⁴

³One cannot avoid defining these relations and operations directly on the states. To see this let the operator \tilde{N} satisfy $\tilde{N}|\gamma, 0, h, s\rangle_{k,g} = N(\gamma, s)|\gamma, 0, h, s\rangle_{k,g}$ where $N(\gamma, s)$ is supposed to be the number represented by $|\gamma, 0, h, s\rangle_{k,g}$. Because of the possible presence of leading and trailing 0s, the eigenspaces of \tilde{N} are infinite dimensional. One knows that the set of eigenvalues of \tilde{N} satisfy the relevant axioms. To prove that $N(\gamma, s)$ is the number represented by $|\gamma, 0, h, s\rangle_{k,g}$ one must show that \tilde{N} is a homomorphism. This requires defining the arithmetic relations and operations directly on the states and showing that they satisfy the relevant axioms.

⁴That is, for all j , If j is in both $[l, u]$ and $[l', u']$, then $s(j, h) = s'(j, h')$. If j is in $[l, u]$ and not in $[l', u']$, then $s(j, h) = 0$. If j is in $[l', u']$ and not in $[l, u]$, then $s'(j, h') = 0$. The domains of s and s' are $[l, h; u, h]$ and $[l', h'; u', h']$.

Arithmetic ordering $<_{A,k,g}$ on N , and on positive I and Ra states,

$$(5) \quad |+, 0, h, s\rangle_{k,g} <_{A,k,g} |+, 0, h', s'\rangle_{k,g}$$

expresses the condition that the left hand state is arithmetically less than the right hand state.⁵ The extension to zero and negative I and Ra states is given by the two conditions

$$(6) \quad \begin{aligned} &|+, 0, h, \bar{0}\rangle_{k,g}, <_{A,k,g} |+, 0, h', s'\rangle_{k,g} \text{ for all } s' \neq \bar{0} \\ &|+, 0, h, s\rangle_{k,g} <_{A,k,g} |+, 0, h', s'\rangle_{k,g} \\ &\quad \rightarrow |-, 0, h', s'\rangle_{k,g} <_{A,k,g} |-, 0, h, s\rangle_{k,g}. \end{aligned}$$

Here $\bar{0}$ denotes a constant 0 sequence.

The A subscript in these relations emphasizes that these are arithmetic relations on the states. They are quite different from the usual quantum mechanical relations between states. For instance, two states which differ by the number of leading or trailing 0s are arithmetically equal but are not quantum mechanically equal.

The basic arithmetic operations on Ra are $+$, $-$, \times , and a set of division operations, \div_ℓ , one for each ℓ . This expresses the fact that the set of k -ary rational string numbers is not closed under division when restricted to single finite length strings. However it is closed under division to any finite accuracy, $k^{-\ell}$. For each k , unitary operators for $+$, $-$, \times , and \div_ℓ are represented by $\tilde{+}_{A,k,g}$, $\tilde{-}_{A,k,g}$, $\tilde{\times}_{A,k,g}$, and $\tilde{\div}_{A,k,g,\ell}$. These operators, acting on pairs of q_k string states as input, generate an output triple consisting of the pair of input states and a result string state.

To express this in a bit more detail, let $\tilde{O}_{A,k,g}$ represent any of the four operation types, ($O = +, -, \times, \div_\ell$.) Then

$$(7) \quad \begin{aligned} &\tilde{O}_{A,k,g} |\gamma, 0, h, s\rangle_{k,g} |\gamma', 0, h', s'\rangle_{k,g} \\ &= |\gamma, 0, h, s\rangle_{k,g} |\gamma', 0, h', s'\rangle_{k,g} |\gamma'', 0, h'', s''\rangle_{k,g,O_A} \end{aligned}$$

The preservation of the input states is sufficient to ensure that the operators are unitary. The values of h, h', h'' are arbitrary except that they are all different.

In these equations the states $|\gamma'', 0, h'', s''\rangle_{k,g}$ with subscripts $O = +, -, \times, \div_\ell$ give the results of the arithmetic operations. It is often useful to write them as

$$(8) \quad \begin{aligned} &|\gamma'', 0, h'', s''\rangle_{k,g,+} = |0, h'', (\gamma', s' +_A \gamma, s)\rangle_{k,g}, \\ &|\gamma'', 0, h'', s''\rangle_{k,g,-} = |0, h'', (\gamma', s' -_A \gamma, s)\rangle_{k,g}, \\ &|\gamma'', 0, h'', s''\rangle_{k,g,\times} = |0, h'', (\gamma', s' \times_A \gamma, s)\rangle_{k,g}, \\ &|\gamma'', 0, h'', s''\rangle_{k,g,\div_\ell} = |0, h'', (\gamma', s' \div_{A,\ell} \gamma, s)\rangle_{k,g}. \end{aligned}$$

The subscript A on these operations distinguishes them as arithmetic operations. They are different from the quantum operations of linear superposition, $+$, $-$ and product, \times with no subscripts.

⁵The $<_{A,k}$ relation can be expressed by conditions on s and s' . Let j_{max} and j'_{max} be the largest j values such that $s(j_{max}, h) > 0$ and $s'(j'_{max}, h') > 0$. Then $|+, 0, h, s\rangle_{k,g} <_{A,k,g} |+, 0, h', s'\rangle_{k,g}$ if $j_{max} < j'_{max}$ or $j_{max} = j'_{max}$ and $s(j_{max}, h) < s'(j'_{max}, h')$.

Extension of these operations to linear superposition states introduces entanglement. Use of Eq. 7 gives

$$(9) \quad \tilde{O}_{A,k,g}\psi\psi' = \sum_{\gamma,h,s} \sum_{\gamma',h',s'} k_{k,g} \langle \gamma, 0, h, s | \psi \rangle_{k,g} \langle \gamma', 0, h', s' | \psi' \rangle_{k,g} \\ \times |\gamma, 0, h, s\rangle_{k,g} |\gamma', 0, h', s'\rangle_{k,g} |\gamma'', 0, h'', s''\rangle_{k,g, O_A}.$$

Another operation that is essential for the axioms for N and is useful for the others is that of the successor operation which corresponds to the $+1$ operation. For q_k string states the definition can be expanded to include successor operators \tilde{V}_j for each integer j . The action of \tilde{V}_j on a base k string state

$$(10) \quad \tilde{V}_j |\gamma, 0, h, s\rangle_{k,g} = |\gamma', 0, h, s'\rangle_{k,g}$$

corresponds to the arithmetic addition of k^j where j is any integer. The usefulness of this operation is that the other arithmetic operations can be defined in terms of it.

Also this definition provides an efficient way⁶ to implement the arithmetic operations [34]. This follows from the observations that for each k

$$(11) \quad \tilde{V}_j^k = \tilde{V}_{j+1}$$

and that the implementation of each \tilde{V}_j is efficient. Also implementation of the various arithmetic operations by use of the \tilde{V}_j is efficient.

2.2. Transformations of Representations. As was noted earlier, the Fock space, \mathcal{F}_k , is spanned by the basis, $\mathcal{B}_{k,g}$, that is the set of all finite tuples of states of finite q_k strings. Ultimately, $\mathcal{B}_{k,g}$ consists of sums and products of the individual q_k bases, $\mathcal{B}_{k,h,j,g}$ where $\mathcal{B}_{k,h,j,g}$ is a set of k single q_k states that spans the k dimensional Hilbert space $\mathcal{H}_{j,h}$ for site j, h .

As is well known there are an infinite number of choices for a basis set in a Hilbert space. Here $\mathcal{B}_{k,h,j,g}$ denotes one choice. A choice of a basis set for each $\mathcal{H}_{j,h}$ is equivalent to a gauge fixing. Thus a basis choice for each j, h corresponds to a particular gauge choice at j, h . The subscript g represents a gauge fixing function where for each integer pair j, h ,

$$(12) \quad g(j, h) = \mathcal{B}_{k,j,h,g}.$$

In what follows it is quite useful to treat $\mathcal{B}_{k,g}$ and \mathcal{F}_k together. They will be denoted as $\mathcal{FB}_{k,g}$. One reason for this is that the arithmetic relations and operations, which are needed to prove that the states $|\gamma, 0, h, s\rangle_{k,g}$ represent numbers, in N , I , and Ra , are defined on the states in $\mathcal{B}_{k,g}$ and extend by linearity to states in \mathcal{F}_k .

The arguments given so far show that the set of all $\mathcal{FB}_{k,g}$ form a space parameterized by a space of 2-tuples (k, g) . Here k is a base and g is a gauge fixing function defined by Eq. 12. Transformations $(k, g) \rightarrow (k', g')$ on the parameter space induce transformations $\mathcal{FB}_{k,g} \rightarrow \mathcal{FB}_{k',g'}$ on the representation space. The two transformations of interest are the k changing transformations $\tilde{W}_{k',k}$ and the gauge transformations U_k . Gauge transformations of the sign qubit are ignored here although they could be easily included.

⁶The numbers of steps to implement the arithmetic operations are polynomial in the qubit string lengths.

The gauge transformation, U_k is a $U(k) = U(1) \times SU(k)$ valued function on $I \times I$. U_k is global if $U_k(j, h)$ is independent of j, h . Otherwise it is local. The action of U_k changes the basis set or state reference frame for each qukit [31] in that

$$(13) \quad U_k(j, h)B_{k,j,h,g} = B_{k,j,h,g'}.$$

holds for each g .

One can use the definition of U_k to define gauge transformation operators on $\mathcal{B}_{k,h,g}$ and $\mathcal{B}_{k,g}$. Here notation will be abused in that U_k will represent all these transformations. It will be clear from context which is meant.

The action of U_k on a state $|\gamma, 0, h, s, \rangle_{k,g}$ and the individual A-C operators is given by

$$(14) \quad \begin{aligned} |\gamma, 0, h, s\rangle_{k,g'} &= U_k|\gamma, 0, h, s\rangle_{k,g} \\ &= c_{\gamma,0,h}^\dagger U_k(u, h)(a_k^\dagger)_{s(u),u,h} \cdots U_k(l, h)(a_k^\dagger)_{s(l),l,h}|0\rangle \\ &= c_{\gamma,0,h}^\dagger ((a_k^\dagger)_{U_k(u,h)})_{s(u),u,h} \cdots ((a_k^\dagger)_{U_k(l,h)})_{s(l),l,h}|0\rangle \end{aligned}$$

where

$$(15) \quad \begin{aligned} ((a_k^\dagger)_{U_k(j,h)})_{\alpha,j,h} &= U_k(j, h)(a_k^\dagger)_{\alpha,j,h} = \sum_\beta U_k(j, h)_{\alpha,\beta} (a_k^\dagger)_{\beta,j,h} \\ ((a_k)_{U_k(j,h)})_{\beta,j,h} &= (a_k)_{\beta,j,h} U_k^\dagger(j, h) = \sum_\alpha U_k^*(j, h)_{\alpha,\beta} a_{\alpha,j,h} \end{aligned}$$

These results are based on the representation of $U_k(j, h)$ as

$$(16) \quad U_k(j, h) = \sum_{\alpha,\beta} (U_k(j, h))_{\alpha,\beta} (a_k^\dagger)_{\alpha,j,h} (a_k)_{\beta,j,h}.$$

Here $((a_k^\dagger)_{U_k(j,h)})_{\alpha,j,h}$ is the creation operator for q_k in the state $|\alpha, j, h\rangle_{k,g'}$ in the basis $B_{k,j,h,g'}$ just as $(a_k^\dagger)_{\alpha,j,h}$ is the creation operator for q_k in the state $|\alpha, j, h\rangle_{k,g}$ in the basis $B_{k,j,h,g}$.

The base changing operator $\tilde{W}_{k',k}$ is more complex. If $\tilde{W}_{k',k}$ is defined on the state $|\gamma, 0, h, s\rangle_{k,g}$, then

$$(17) \quad |\gamma, 0, h, s'\rangle_{k',g} = \tilde{W}_{k',k}|\gamma, 0, h, s\rangle_{k,g}$$

represents the same number in the base k' representation as $|\gamma, 0, h, s\rangle_k$ does in the base k representation. This a nontrivial requirement because one needs to specify what is meant by "the same number as". In particular it means that all number theoretic properties are valid for $|\gamma, 0, h, s\rangle_k$, if and only if they are valid for $|\gamma, 0, h, s'\rangle_{k'}$.

For any k', k , the operator $\tilde{W}_{k',k}$ is defined for all natural number and integer qukit string states. For qukit string states that represent rational numbers the domain and range of $\tilde{W}_{k',k}$ depend on the relations between the prime factors of k and k' . The domains and ranges for the different cases are summarized by the

following relations [29]. Let $PF(k)$ denote the prime factors of k . Then

$$\begin{aligned}
 & \text{If } PF(k) \cap PF(k') = 0 \text{ then the domain and range of } \tilde{W}_{k',k} \\
 & \quad \text{are the integer subspaces of } \mathcal{FB}_{k,g} \text{ and } \mathcal{FB}_{k',g} \\
 & \text{If } PF(k) \subset PF(k') \text{ then } \tilde{W}_{k',k} \mathcal{FB}_{k,g} \subset \mathcal{FB}_{k',g}, \\
 (18) \quad & \text{If } PF(k) \supset PF(k') \text{ then } \tilde{W}_{k',k} \mathcal{FB}_{k,g} = \mathcal{FB}_{k',g}, \\
 & \text{If } PF(k), PF(k') \text{ each have elements not in the other and} \\
 & \quad \text{share elements in common, then } \tilde{W}_{k',k} \mathcal{FB}_{k,g} = \mathcal{FB}_{k',g}, \\
 & \text{If } PF(k) = PF(k') \text{ then } \tilde{W}_{k',k} \mathcal{FB}_{k,g} = \mathcal{FB}_{k',g}.
 \end{aligned}$$

In the above $\subset \mathcal{FB}_{k,g}$ denotes a subspace of $\mathcal{FB}_{k,g}$ that contains the integer representations. In all these cases, if the state $|\gamma, 0, h, s\rangle_{k,g}$ is in the domain of $\tilde{W}_{k',k}$, then the base k' state, $\tilde{W}_{k',k}|\gamma, 0, h, s\rangle_{k,g}$, represents the same rational number as does $|\gamma, 0, h, s\rangle_{k,g}$.

The case where $PF(k) = PF(k')$ is of special interest because for each k there is a smallest k' that has the same prime factors as k . If

$$(19) \quad k = p_{j_1}^{h_1} \cdots p_{j_n}^{h_n},$$

then the smallest k' is given by

$$(20) \quad k' = p_{j_1} \cdots p_{j_n}.$$

Here p_{j_a} for $a = 1, 2, \dots, n$ is the j_a th prime number. This shows that for each finite subset S of primes, there is a set $[k_S]$ of bases such that for any pair $k, k' \in [k_S]$, $\tilde{W}_{k',k}$ is defined everywhere on $\mathcal{FB}_{k,g}$ and $\tilde{W}_{k',k} \mathcal{FB}_{k,g} = \mathcal{FB}_{k',g}$.

A special case of this consists of the values k_n whose factors are the first n primes, each to the first power,

$$(21) \quad k_n = p_1 p_2 \cdots p_n = 2 \times 3 \times \cdots \times p_n.$$

The sets $[k_n]$ are of interest here because, if $n < m$, then $[k_n] \subset [k_m]$. The limit properties, as $n \rightarrow \infty$, of $[k_n]$ and \tilde{W}_{k',k_n} are open for investigation.

It should also be noted that the definitions of both U_k and $\tilde{W}_{k',k}$ extend by linearity to linear superpositions of qukit string states. If

$$\psi = \sum_{\gamma, h, s} c_{\gamma, h, s} |\gamma, 0, h, s\rangle_{k, g},$$

then

$$\begin{aligned}
 (22) \quad U_k \psi &= \sum_{\gamma, h, s} c_{\gamma, h, s} U_k |\gamma, 0, h, s\rangle_{k, g} \\
 \tilde{W}_{k',k} \psi &= \sum_{\gamma, h, s} c_{\gamma, h, s} \tilde{W}_{k',k} |\gamma, 0, h, s\rangle_{k, g}.
 \end{aligned}$$

The validity of the second equation is restricted to the case where all component states with nonzero coefficients are in the domain of $\tilde{W}_{k',k}$.

It is of interest to note that there is in general no commutation relation between U_k and $\tilde{W}_{k,k'}$. The one exception is the case when $k' = k^n$ for some n . However, for each pair k, k' for which $\tilde{W}_{k,k'}$ is defined everywhere on \mathcal{F}_k , and for each pair $U_k, U_{k'}$ one can define a transformed operator

$$(23) \quad (\tilde{W}_{U',U})_{k',k} = U_{k'}' \tilde{W}_{k',k} U_k^\dagger.$$

This operator takes a transformed state $U_k|\gamma, h, s\rangle_{k,g}$ to a base k' state

$$(\tilde{W}_{U',U})_{k',k}U_k|\gamma, h, s\rangle_{k,g} = U_{k'}'\tilde{W}_{k',k}|\gamma, h, s\rangle_{k,g}$$

that represents the same number in the k', g' representation as $|\gamma, h, s\rangle_{k,g}$ does in the k, g representation. The steps in the representation transformations are

$$(24) \quad (k, g) \xrightarrow{U_k} (k, g_1) \xrightarrow{\tilde{W}_{k,k'}} (k', g_1) \xrightarrow{U_{k'}'} (k', g').$$

Note that basis or gauge choice g_1 chosen for the base k states is used to label the gauge choice for base k' states that are connected by $\tilde{W}_{k,k'}$.

2.3. Transformations of Arithmetic Relations and Operations. The arithmetic relations and operations transform in the expected way under the action of $\tilde{W}_{k,k'}$ and U_k . One has

$$(25) \quad \begin{aligned} &=_{A,k',g} = (\tilde{W}_{k,k'} =_{A,k,g} \tilde{W}_{k,k'}^\dagger) \\ &\leq_{A,k',g} = \tilde{W}_{k,k'} \leq_{A,k,g} \tilde{W}_{k,k'}^\dagger \end{aligned}$$

for the relations and

$$(26) \quad \begin{aligned} &O_{A,k',g} = \tilde{W}_{k,k'} \times \tilde{W}_{k,k'} \times \tilde{W}_{k,k'} \\ &\times O_{A,k,g} \tilde{W}_{k,k'}^\dagger \times \tilde{W}_{k,k'}^\dagger \end{aligned}$$

for $O = +, \times, -, \div_\ell$.

These transformations of relations and operations hold without restrictions if and only if k and k' have the same prime factors. If this is not the case, then the restrictions expressed by Eq. 18 apply here. In the worst case where k and k' are relatively prime, the transformations are restricted to the integer subspaces of \mathcal{F}_k and $\mathcal{F}_{k'}$. The presence of three transformation operators on the left of $O_{A,k,g}$ and two to the right accounts for the fact that $O_{A,k,g}$ preserves the two input strings and creates a third.

One has similar relations for the gauge transformations of relations and operations.

$$(27) \quad \begin{aligned} &=_{A,k,g'} = (U_k =_{A,k,g} U_k^\dagger) \\ &\leq_{A,k',g} = U_k \leq_{A,k,g} U_k^\dagger \end{aligned}$$

for the relations and

$$(28) \quad \begin{aligned} &O_{A,k,g'} = U_k \times U_k \times U_k \\ &\times O_{A,k,g} U_k^\dagger \times U_k^\dagger \end{aligned}$$

for $O = +, \times, -, \div_\ell$.

2.4. Unary Representations. So far all number bases have been considered except one, the value $k = 1$. The $k = 1$ string representations are called unary representations. These are not usually considered, because basic arithmetic operations on these numbers are exponentially hard. For instance the number of steps needed to add two unary numbers is proportional to the values of the numbers and not to the logarithms of the values. However, even though they are not used arithmetically, they are always present in an interesting way.

To see this one notes that $k = 1$ representations are the only ones that are extensive, all others are representational. The representational property for $k \geq 2$

base states of a qukit string means that a number represented by a state has nothing to do with the properties of the string state. The number represented by the state, $|672\rangle$, of a string of 3 q'_{10} s is unrelated to the properties of the qukits in the state.

The extensiveness of a unary representation means that any collection of systems is an unary representation of a number that is the number of systems in the collection. There are many examples. A system of spins on a lattice is an unary representation of a number, that is the number of spins in the system. A gas of particles in a box is an unary representation of a number, that is the number of particles in the box. The qukit strings that play such an important role in this paper are unary representations of numbers, that are the number of qukits in the strings. A single qukit is an unary representation of the number 1.

The omnipresence of unary representations relates to another observation that 1 is the only number that is a common factor of all prime numbers and of all numbers. So it is present as a factor of any base. This ties in with the fact that unary representations of numbers are possible only for natural numbers and integers.⁷ Also there is the related observation that, for any pair k, k' , the domain and range of $\tilde{W}_{k',k}$ include the integer subspaces of \mathcal{F}_k and $\mathcal{F}_{k'}$, and if k, k' have no prime factors in common, \mathcal{F}_k and $\mathcal{F}_{k'}$ are the domain and range of $\tilde{W}_{k',k}$.

The extensiveness of unary representations supports the inclusion of the $U(1)$ factor in the definition of U_k as a $U(1) \times SU(k)$ valued function on $I \times I$. As a very simple example, a state $(a_k^\dagger)_{\alpha,(i,j)}|0\rangle$ of a qukit at location (i, j) is an unary representation of the number 1. Multiplication of this state by a phase factor $e^{i\theta_{i,j}}$ is a transformation that gives another state that is also an unary representation of the number 1.

This argument extends to states of strings of qukits. A phase factor associated with any state of a string of q_k at sites $(l, h), \dots (u, h)$ is a product of the phase factors associated with each of the q_k in the string. If $e^{i\theta_{j,h}}$ is a phase factor for the state of the q_k at site (j, h) , then $e^{i\Theta_{[(l,h),(u,h)]}}$, where $\Theta_{[(l,h),(u,h)]} = \sum_{j=l}^u \theta_{j,h}$, is the phase factor for the state of the q_k string in the site interval $[(l, h), (u, h)]$.

As is well known, multiplying any state by a phase factor gives the same state as far as any physical meaning is concerned. However here one can have linear superpositions of states of strings of q_k both at different locations and of different length strings. In these cases the phase factors do matter to the extent that they can change the relative phase between the components in the superposition.

2.5. Composite and Elementary Qukits. So far the qukit components of strings are considered to be different systems for each value of k . A k qukit is different from a k' qukit just as a spin k system is different from a spin k' system. This leads to a large number of different qukit types, one for each value of k . However, the dependence of the properties of the base changing operator $\tilde{W}_{k',k}$ on the prime factors of k and k' suggests that instead one consider qukits q_k as composites q_{c_k} of prime factor qukits q_{p_n} . In general the relation between the base

⁷Non integer rational numbers require pairs of unary representations. However, pairs are not being considered here.

k q_k and the composite base $c(k)$ q_{c_k} is given by

$$(29) \quad q_{c_k} = q_{p_{j_1}}^{h_1} q_{p_{j_2}}^{h_2} \cdots q_{p_{j_n}}^{h_n}.$$

where (Eq. 19)

$$k = p_{j_1}^{h_1} p_{j_2}^{h_2} \cdots p_{j_n}^{h_n}$$

. Simple examples of this for $k = 10$ and 18 are $q_{c_{10}} = q_2 q_5$ and $q_{c_{18}} = q_2 q_3 q_3$.

The observation that for each k there is a smallest k' with the same prime factors and its relevance to the properties of $\tilde{W}_{k',k}$ suggest the importance of the $q_{c_{k'}}$ where the powers of the prime factors are all equal to 1 (Eq. 20)

$$(30) \quad q_{c_{k'}} = q_{p_{j_1}} q_{p_{j_2}} \cdots q_{p_{j_n}}.$$

A particular example of this for k_n , the product of the first n prime numbers, is shown by (Eq. 21)

$$(31) \quad q_{c_{k_n}} = q_2 q_3 q_5 \cdots q_{p_n}.$$

These considerations suggest a change of emphasis in that one should regard prime number qukits q_{p_n} as basic or elementary and the qukits q_k as composites of the elementary ones. In this case one would want to consider possible physical properties of the elementary qukits and how they interact and couple together to form composites. This is a subject for future work. It is, however, intriguing to note that if the prime number q_{p_n} are considered as spin systems with spin s_n given by $2s_n + 1 = p_n$, then there is just one fermion, q_2 . All the others are bosons.

As was the case for strings of q_k , one wants to represent numbers by states of finite strings of composite q_{c_k} . In general, this involves replacing the k dimensional Hilbert space \mathcal{H}_k at each site in $I \times I$ by a product space

$$(32) \quad \mathcal{H}_{c_k} = \mathcal{H}_{p_{j_1}}^{h_1} \otimes \cdots \otimes \mathcal{H}_{p_{j_n}}^{h_n},$$

and then following the development in the previous sections to describe number states. In particular the gauge fixing would apply to each component space in Eq. 32 for each location in $I \times I$.

The requirement that states of the form $|\gamma, 0, h, s'\rangle_{c_{k'},g}$ represent numbers is based on an ordering of the basis states of q_{c_k} , or, what is equivalent, an ordering of the n - *tuples* in the range set of s' . The definitions of arithmetic relations and operations for these states must respect the ordering and they must satisfy the relevant axioms and theorems for the type of number being considered.

The description of the transformation operations $\tilde{W}_{k',k}$ and $U_{k'}$ can be extended to apply to the composite qukit strings. The base changing operator $\tilde{W}_{c_{k'},c_k}$ changes states of q_{c_k} strings to states of $q_{c_{k'}}$ strings that should represent the same number. Note that the expression of $\tilde{W}_{c_{k'},c_k}$ in terms of sums of products of AC operators will include the annihilation of many component elementary qukits in q_{c_k} and creation of many that are components of $q_{c_{k'}}$.

The description of gauge transformations U_{c_k} applied to states of q_{c_k} is interesting. If q_{c_k} is composed of elementary q_{p_j} as given by Eq. 30, then U_{c_k} is a map from $I \times I$ to elements of $U(p_{j_1}) \times \cdots \times U(p_{j_n})$. Here $U(p_{j_i})$ is the unitary group of prime dimension p_{j_i} . For the special case of Eq. 31, $U_{c_{k_n}}$ takes values in

$U(p_1) \times \cdots \times U(p_n)$. respectively. Since $U(p_j) = U(1) \times SU(p_j)$ the values of $U_{c_{k_n}}$ can be represented as elements of

$$(33) \quad \begin{aligned} & U(1) \times SU(p_1) \times SU(p_2) \times \cdots \times SU(p_n) \\ & = U(1) \times SU(2) \times SU(3) \times SU(5) \times \cdots \times SU(p_n). \end{aligned}$$

Here the phase factor elements in $U(1)$ for each elementary qukit have been combined into one phase factor for the composite $q_{c_{k_n}}$.

This brief description of composite and elementary qukits shows that this may be an interesting approach to examine further. Problems to investigate include the nature of the coupling of elementary qukits to form a composite, invariance of properties of composite qukit string states under the action of U_k , particularly of $U_{c(k_n)}$, and other aspects.

The discussion so far suggests that, as far as quantum theory representations of natural numbers, integers, and rational numbers are concerned, it is sufficient to limit components of gauge transformations to products of elements of $U(1)$ and products of elements of $SU(p)$ groups where p is a prime number. Furthermore it is sufficient that, for each prime p , elements of $SU(p)$ occur at most once in the product. It is also sufficient to limit components to products of the form of Eq. 33 for $n = 1, 2, \cdots$ as these will include representations for all rational numbers.

3. Quantum Representations of Real Numbers

Here quantum representations of real numbers are described as equivalence classes of sequences of base $k \geq 2$ qukit (q_k) string states that satisfy the Cauchy condition.⁸ Sequences of states are defined to be functions Ψ from the natural numbers to states in \mathcal{F}_k . If the states in the range set of Ψ are all basis states in $\mathcal{B}_{k,g}$, then $\Psi(n) = |\gamma_n, h_n, s_n\rangle_{k,g}$. The values of h_n in the states $|\gamma_n, h_n, s_n\rangle_k$ are all different in that $m \neq n \rightarrow h_m \neq h_n$. This is needed because one must be able to distinguish $\Psi(n)$ from $\Psi(m)$. Here and from now on the location 0 of the sign qubit in $|\gamma, 0, h, s\rangle_{k,g}$ is suppressed as it is always the same.

These sequences extend classical representations in that the $\mathcal{B}_{k,g}$ valued sequences correspond to classical states of kit sequences. However sequences of linear superposition states have no classical correspondences.

3.1. The Cauchy Condition for State Sequences. The definition of the Cauchy condition for sequences of q_k string states is a translation into quantum mechanics of a definition in mathematical analysis textbooks [26]. To this end let Ψ be a $\mathcal{B}_{k,g}$ valued sequence of q_k string states. The sequence Ψ satisfies the Cauchy condition if

$$(34) \quad \begin{aligned} & \text{For each } \ell \text{ there is a } p \text{ where for all } j, m > p \\ & |(|\Psi(j) -_{A,k,g} \Psi(m)|_{A,k,g})\rangle_{k,g} <_{A,k,g} |+, -\ell\rangle_{k,g}. \end{aligned}$$

Here $|(|\Psi(j) -_{A,k,g} \Psi(m)|_{A,k,g})\rangle_{k,g}$ is the basis state that is the base k arithmetic absolute value of the state resulting from the arithmetic subtraction of $\Psi(m)$ from $\Psi(j)$. The Cauchy condition says that this state is arithmetically less than or equal to the state $|+, -\ell\rangle_{k,g} = |+, 0_{[0, -\ell+1]} 1_{-\ell}\rangle_{k,g}$ for all j, m greater than some p .

⁸This extends earlier work [6] on real number representations that was limited to $k = 2$.

Here $|+, -\ell\rangle$ represents the number $k^{-\ell}$. The subscripts A, k, g are used to indicate that the operations are arithmetic and are defined for base k string states in $\mathcal{B}_{k,g}$. They are not the usual quantum theory operations.⁹

The Cauchy condition can be extended to sequences of linear superpositions of q_k string states. Let $\Psi(n) = \sum_{\gamma,h,s} |\gamma, h, s\rangle_{k,g} \langle \gamma, h, s | \Psi(n) \rangle$. The probability that the arithmetic absolute value of the arithmetic difference between $\Psi(j)$ and $\Psi(m)$ is arithmetically less than or equal to $|+, -\ell\rangle$ is given by

$$(35) \quad P_{j,m,\ell} = \sum_{\gamma,h,s} \sum_{\gamma',h',s'} |\langle \gamma, h, s | \Psi(j) \rangle \langle \gamma', h', s' | \Psi(m) \rangle|^2 : \\ |(|\gamma, h, s -_{A,k,g} \gamma', h', s'|_{A,k,g})_{k,g} \leq_{A,k,g} |+, -\ell\rangle_{k,g}.$$

The sum is over all $|\gamma, h, s\rangle, |\gamma', h', s'\rangle$ that satisfy the statement in the second line of the above equation.

The definition of the probability P^Ψ that Ψ satisfies the Cauchy condition is obtained from the values of $P_{n,m,\ell}^\Psi$ by taking account of the quantifiers in the definition in Eq. 34. To this end define the probabilities $P_{p,\ell}^\Psi$, P_ℓ^Ψ , and P^Ψ by

$$(36) \quad P_{p,\ell}^\Psi = \inf_{n,m > p} P_{n,m,\ell}^\Psi \\ P_\ell^\Psi = \limsup_{p \rightarrow \infty} P_{p,\ell}^\Psi = \lim_{p \rightarrow \infty} P_{p,\ell}^\Psi \\ P_C^\Psi = \liminf_{\ell \rightarrow \infty} P_\ell^\Psi = \lim_{\ell \rightarrow \infty} P_\ell^\Psi.$$

This definition is based on the structure of the Cauchy condition in Eq. 34. It shows that the asymptotic values of $P_{n,m,\ell}^\Psi$ as $m, n \rightarrow \infty$ are important. The values for any particular m, n or finite set $\{m, n\}$ of values (with ℓ fixed) for each ℓ are not important. The structure also shows that $P_{p,\ell}^\Psi$ is a non decreasing function of p and that P_ℓ^Ψ is a non increasing function of ℓ .

The sequence Ψ is said to be a Cauchy sequence if P_Ψ is equal to 1. A necessary and sufficient condition for this to occur is that $P_{n,m,\ell}^\Psi \rightarrow 1$ as $n, m \rightarrow \infty$ for each ℓ . That is,

THEOREM 1. $P_\Psi = 1 \Leftrightarrow \lim_{m,n \rightarrow \infty} P_{n,m,\ell}^\Psi = 1$ for each ℓ .

Proof sufficiency: Obvious as probabilities are bounded above by 1, One has $P_{p,\ell}^\Psi = 1$ for each p and ℓ . This gives $P_\ell^\Psi = 1$ for each ℓ .

necessity: Assume $P_\Psi = q < 1$. From the definition of P_ℓ^Ψ one sees that it approaches q from above as ℓ increases. It follows that for sufficiently large ℓ , $P_{p,\ell}^\Psi$, which is non decreasing is bounded from above by q as p increases. It follows from the definition of $P_{p,\ell}^\Psi$ that either $\lim_{m,n \rightarrow \infty} P_{n,m,\ell}^\Psi$ does not exist or it exists and is $\leq q$. QED

There are many examples of sequences Ψ that are Cauchy with probability 1. A simple example is the following: Let s be a $0, 1, \dots, k-1$ valued function on the non positive integers $[0, -\infty]$. Define $\Psi(n)$ by

$$(37) \quad \Psi(n) = |+, 0, h, s_{[0, -n+1]}\rangle_k \times \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} |-n, h, j\rangle_k.$$

⁹When it is desired to emphasize the dependence of the definition of the Cauchy condition on g , Eq. 34 will be referred to as the g -Cauchy condition.

Here $|j, h, -n\rangle_k$ denotes a q_k at site $-n, h$ in state j .

The sequence Ψ is Cauchy with probability 1 because $P_{n,m,\ell}^\Psi = 1$ for all $m, n > \ell$. Also this example does not correspond to any classical Cauchy sequence of rational numbers. Additional examples are given in [6].

3.2. Basic Relations on State Sequences. One way to proceed is to define the field relations and operations on equivalence classes of sequences and show that these satisfy the real number axioms. However this method does not make clear the relation between the basic arithmetic relations on the q_k string states and those on the equivalence classes. The method used here is to define the basic relations and operations on the sequences in terms of the relations and operations on the q_k string states and use them to define the equivalence classes and field relations and operations on the classes.

As a piece of nomenclature let $Re_{i,S,k,g}$ denote the two relations where $Re_{i,S,k,g}$ is $=_{S,k,g}$ (equality) for $i = 1$ and $Re_{i,S,k,g}$ is $<_{S,k,g}$ (less than) for $i = 2$. The simplest definition one thinks of is an elementwise definition:

$$(38) \quad \Psi(n) Re_{i,S,k,g} \Psi' \Leftrightarrow \forall n \Psi Re_{i,A,k,g} \Psi'(n).$$

Here $Re_{i,A,k,g}$ corresponds to the two relations on finite q_k string states.

These definitions are unsatisfactory in that they are too strong. For $i = 1$ this definition gives the result that for most \mathcal{F}_k valued sequences, Ψ , the probability that $\Psi =_{S,k,g} \Psi$ is 0. This holds even if Ψ is Cauchy. For $i = 2$ the definition of $<_{S,k,g}$ does not have the right asymptotic properties.

A better definition of $=_{S,k,g}$ is an asymptotic definition. Let Ψ and Ψ' be $\mathcal{B}_{k,g}$ valued sequences. Then

$$(39) \quad \Psi =_{\infty,k,g} \Psi' \Leftrightarrow \forall \ell \exists p \forall j, m > p (|\Psi(j) -_{A,k,g} \Psi'(m)|_{A,k,g})_k <_{A,k,g} |+, -\ell\rangle_{k,g}.$$

This definition is the same as the Cauchy condition of Eq. 34 except that $\Psi'(m)$ replaces $\Psi(m)$. This definition says nothing about whether specific elements of Ψ equal the corresponding ones of Ψ' . It says that the elements of Ψ and Ψ' must approach each other asymptotically. It is easy to show that this definition satisfies the requirement for a definition of equality. It is reflexive, symmetric, and transitive.

An asymptotic definition of ordering is given by

$$(40) \quad \Psi <_{\infty,k,g} \Psi' \Leftrightarrow \exists \ell \exists p \forall j, m > p |\Psi'(j) -_{A,k,g} \Psi(m)|_k >_{A,k,g} |+, -\ell\rangle_k.$$

This is also an asymptotic definition in that it says that Ψ is less than Ψ' if Ψ is asymptotically arithmetically less than Ψ' by some fixed amount, $|+, -\ell\rangle_k$. This definition differs from Eq. 39 in that $\forall \ell$ is replaced by $\exists \ell$, there is no arithmetic absolute value, and $<_{A,k,g}$ is replaced by $>_{A,k,g}$.

These definitions can be extended to $\mathcal{F}_{j,k}$ valued sequences. Let Ψ and Ψ' be sequences of this type. Define $P_{n,m,\ell}^{\Psi=\infty\Psi'}$ by,

$$(41) \quad P_{n,m,\ell}^{\Psi=\infty\Psi'} = \sum_{\gamma,h,s} \sum_{\gamma',h',s'} |d_{\gamma,h,s}^n f_{\gamma',h',s'}^m|^2 : \\ |(|(\gamma, h, s) -_{A,k,g} (\gamma', h', s')|_{A,k,g})_k \leq_{A,k,g} |+, -\ell\rangle_k$$

where

$$(42) \quad \begin{aligned} d_{\gamma,h,s}^n &= \langle \gamma, h, s | \Psi(n) \rangle \\ f_{\gamma',h',s'}^m &= \langle \gamma', h', s' | \Psi'(m) \rangle. \end{aligned}$$

Here $P_{n,m,\ell}^{\Psi=\infty\Psi'}$ is the probability that $\Psi(n)$ and $\Psi'(m)$ satisfy the relation in the second line of Eq. 41.

Let $P^{\Psi=\infty\Psi'}$ be the probability that $\Psi =_{\infty} \Psi'$, i. e. that Ψ equals Ψ' S asymptotically. Here $P^{\Psi=\infty\Psi'}$ is given by

$$(43) \quad \begin{aligned} P_{p,\ell}^{\Psi=\infty\Psi'} &= \inf_{n,m>p} P_{n,m,\ell}^{\Psi=\infty\Psi'} \\ P_{\ell}^{\Psi=\infty\Psi'} &= \limsup_{p \rightarrow \infty} P_{p,\ell}^{\Psi=\infty\Psi'} = \lim_{p \rightarrow \infty} P_{p,\ell}^{\Psi=\infty\Psi'} \\ P^{\Psi=\infty\Psi'} &= \liminf_{\ell \rightarrow \infty} P_{\ell}^{\Psi=\infty\Psi'} = \lim_{\ell \rightarrow \infty} P_{\ell}^{\Psi=\infty\Psi'}. \end{aligned}$$

These equations are similar to those in Eq. 36 because the quantifier setup in Eq. 39 is the same as that for the Cauchy condition in Eq. 34. As was the case before, $P_{p,\ell}^{\Psi=\Psi'}$ is a non decreasing function of p for each ℓ and $P_{\ell}^{\Psi=\Psi'}$ is a non increasing function of ℓ .

A similar result holds for the probability $P^{\Psi<\infty\Psi'}$ that Ψ is asymptotically less than Ψ' . Eqs. 40 and 42 give

$$(44) \quad \begin{aligned} P_{n,m,\ell}^{\Psi<\infty\Psi'} &= \sum_{\gamma,h,s} \sum_{\gamma',h',s'} |d_{\gamma,h,s}^n f_{\gamma',h',s'}^m|^2 : \\ &|(\gamma', h', s') -_{A,k,g} (\gamma, h, s)\rangle_{k,g} \geq_{A,k,g} |+, -\ell\rangle_{k,g}. \end{aligned}$$

From Eq. 40 one obtains results for $P^{\Psi<\infty\Psi'}$ that are different from Eq. 43:

$$(45) \quad \begin{aligned} P_{p,\ell}^{\Psi<\infty\Psi'} &= \inf_{n,m>p} P_{n,m,\ell}^{\Psi<\infty\Psi'} \\ P_{\ell}^{\Psi<\infty\Psi'} &= \limsup_{p \rightarrow \infty} P_{p,\ell}^{\Psi<\infty\Psi'} = \lim_{p \rightarrow \infty} P_{p,\ell}^{\Psi<\infty\Psi'} \\ P^{\Psi<\infty\Psi'} &= \limsup_{\ell \rightarrow \infty} P_{\ell}^{\Psi<\infty\Psi'} = \lim_{\ell \rightarrow \infty} P_{\ell}^{\Psi<\infty\Psi'}. \end{aligned}$$

These definitions have some satisfying properties. One is that if Ψ and Ψ' are Cauchy sequences then exactly one of the following relations is true with probability 1 and the other two are false (true with probability 0):

$$(46) \quad \begin{aligned} \Psi &=_{\infty,k,g} \Psi' \\ \Psi &<_{\infty,k,g} \Psi' \\ \Psi &>_{\infty,k,g} \Psi' \end{aligned}$$

This result follows from the observation that 0, 1 are the only possible values for $P_{\Psi Re_{i,\infty,k,g}\Psi'}$ for \mathcal{F}_k valued sequences, Ψ, Ψ' , provided that Ψ and Ψ' are both Cauchy. That is

$$(47) \quad \Psi \text{ and } \Psi' \text{ are Cauchy} \Rightarrow P_{\Psi Re_{i,\infty,k,g}\Psi'} = 0 \text{ or } 1.$$

To see this it is sufficient to examine $=_{\infty,k,g}$ as the proofs for the other two relations are similar. One can rewrite Eq. 41 in the equivalent form

$$(48) \quad P_{n,m,\ell}^{\Psi=\infty\Psi'} = \sum_{\gamma,h,s} \sum'_{\gamma',h',s'} |d_{\gamma,h,s}^n|^2 |f_{\gamma',h',s'}^m|^2.$$

The prime on the γ', h', s' sum mean that the sum is restricted to states $|\gamma', h', s'\rangle$ that are at least as large as $|(g, h, s) -_A (+, -\ell)\rangle$ and no larger than $|(g, h, s) +_A$

$(+, -\ell)\rangle$. Since the states Ψ and Ψ' are Cauchy, the distributions $|d_{\gamma,h,s}^n|^2$ and $|f_{\gamma',h',s'}^m|^2$ become increasingly narrow as n, m increase.

The distributions either lie on top of one another for each ℓ or they do not. In the first case, for sufficiently large m, n the restrictions on the γ', h', s' sum can be ignored and $\lim_{m,n \rightarrow \infty} P_{n,m,\ell}^{\Psi=\infty\Psi'} = 1$ for all ℓ . In the second case there is some ℓ for which the state $|+, -\ell\rangle$ approximately separates the distributions. For this and all larger ℓ values, the overlap probability $P_{n,m,\ell}^{\Psi=\infty\Psi'}$ in Eq. 48 approaches 0 as $m, n \rightarrow \infty$.

Another useful property of the asymptotic relation $=_\infty$ is that for each \mathcal{F}_k valued Cauchy sequence Ψ there is a $\mathcal{B}_{k,g}$ valued sequence Ψ' such that $P^{\Psi=\infty\Psi'} = 1$ and Ψ' is Cauchy. The definition of Ψ' and proof that Ψ' is Cauchy and are summarized here. The proof that $P^{\Psi=\infty\Psi'} = 1$, or that $\Psi =_\infty \Psi'$, will not be given as it is similar to that for the Cauchy property of Ψ' .

Define $\Psi'(n) = |\gamma_n, h_n, s_n\rangle_{k,g}$ to be the state that maximizes the probability $P_{n,l}^\Psi(\gamma', h', s')$ where

$$(49) \quad P_{n,l}^\Psi(\gamma', h', s') = \sum_{\gamma,h,s} |d_{\gamma,h,s}^n|^2 : \\ ||(\gamma, h, s) -_{A,k,g} (\gamma', h', s')|_{A,k,g}\rangle_k \leq_{A,k,g} |+, \ell\rangle_{k,g}.$$

Define $Q_{n,\ell}^\Psi$ to be that maximum:

$$(50) \quad Q_{n,\ell}^\Psi = P_{n,l}^\Psi(\gamma_n, h_n, s_n).$$

Since $Q_{n,\ell}^\Psi \geq P_{n,l}^\Psi(\gamma', h', s')$, multiplying both sides by $|d_{\gamma',h',s'}^m|^2$ and carrying out the sum $\sum_{\gamma',h',s'}$ gives

$$(51) \quad Q_{n,\ell}^\Psi \geq P_{n,m,l}^\Psi.$$

Since Ψ is Cauchy,

$$(52) \quad \lim_{n \rightarrow \infty} Q_{n,\ell}^\Psi = 1.$$

To show that Ψ' is Cauchy, it is sufficient to prove that $\lim_{m,n \rightarrow \infty} W_{m,n,\ell} = 0$ where

$$W_{m,n,\ell} = \sum_{\gamma,h,s} \sum_{\gamma',h',s'} |d_{\gamma,h,s}^n|^2 |d_{\gamma',h',s'}^m|^2 : \\ ||(\gamma_n, h_n, s_n) -_{A,k,g} (\gamma_m, h_m, s_m)|_{A,k,g}\rangle >_{A,k,g} |+, -3\ell\rangle_{k,g}.$$

If the condition is true, then $\lim_{m,n \rightarrow \infty} W_{m,n,\ell} = 1$; if it is false, then $\lim_{m,n \rightarrow \infty} W_{m,n,\ell} = 0$.

Also $|+, -3\ell\rangle_{k,g} = |+, -\ell\rangle_{k,g} +_A |+, -\ell\rangle_{k,g} +_A |+, -\ell\rangle_{k,g}$.

Define $X_{m,n,\ell}$ by

$$X_{m,n,\ell} = \sum_{\gamma,h,s} \sum_{\gamma',h',s'} |d_{\gamma,h,s}^n|^2 |d_{\gamma',h',s'}^m|^2 : \\ ||(\gamma_n, h_n, s_n) -_A (\gamma, h, s)|_A\rangle +_A ||(\gamma, h, s) -_A (\gamma', h', s')|_A\rangle \\ +_A ||(\gamma', h', s') -_A (\gamma_m, h_m, s_m)|_A\rangle >_A |+, -3\ell\rangle_{k,g}.$$

(Subscripts k, g are suppressed here.) Since

$$||(\gamma_n, h_n, s_n) -_A (\gamma_m, h_m, s_m)|_A\rangle \\ \leq_A ||(\gamma_n, h_n, s_n) -_A (\gamma, h, s)|_A\rangle +_A ||(\gamma, h, s) -_A (\gamma', h', s')|_A\rangle , \\ +_A ||(\gamma', h', s') -_A (\gamma_m, h_m, s_m)|_A\rangle$$

one has the result that

$$(53) \quad W_{m,n,\ell} \leq X_{m,n,\ell}.$$

The condition in the definition of $X_{m,n,\ell}$ is satisfied only if at least one of the component states is $\geq_A |+, -\ell\rangle$. If this holds for the first or third component, then $X_{m,n,\ell} \leq 1 - Q_{n,\ell}$ or $X_{m,n,\ell} \leq 1 - Q_{m,\ell}$. If it holds for the second component, then $X_{m,n,\ell} \leq 1 - P_{m,\ell}^\Psi$.

Eq. 52 and the fact that Ψ is Cauchy gives the result that $\lim_{m,n \rightarrow \infty} X_{m,n,\ell} = 0$. It follows from Eq. 53 that $\lim_{m,n \rightarrow \infty} W_{m,n,\ell} = 0$. This gives the final result that $|(\gamma_m, h_m, s_m) -_A (\gamma_n, h_n, s_n)|_A \leq_A |+, -\ell\rangle$ and thus that Ψ' is Cauchy.

3.3. Basic Operations on State Sequences. The problems requiring the definition of asymptotic relations do not appear to be present in the definition of basic relations on the sequences. For $\mathcal{B}_{k,g}$ valued sequences Ψ and Ψ' one uses Eqs. 7 and 8 to define $O_{\nu,S,k,g}$ by

$$(54) \quad O_{\nu,S,k,g} \Psi \Psi' = \Theta$$

where for $\nu = 1, 2, 3$ and each n ,

$$(55) \quad \Theta(n) = \Psi(n) \times \Psi'(n) \times \Psi''(n)$$

and

$$(56) \quad \Psi''(n) = \Psi(n) O_{\nu,A,k,g} \Psi'(n).$$

The product structure of the elements of Θ allows one to write

$$(57) \quad \Theta = \Psi \Psi' \Psi''$$

as the product of 3 state sequences.

For $\nu = 4$ one division operator, $\div_{S,k,g}$, can be defined as an operator that is diagonal in the infinite number of state division operators, $\div_{A,\ell}$. One has

$$(58) \quad \div_{S,k,g} \Psi \Psi' = \Psi \Psi' \Psi''$$

where

$$(59) \quad \Psi''(n) = \Psi(n) \div_{A,k,g,n} \Psi'(n).$$

Note the subscript n in $\div_{A,k,g,n}$.

Application of this definition to more general \mathcal{F}_k valued sequences Ψ and Ψ' generates a single sequence Θ of entangled states that cannot be represented in the product form of Eq. 57. From Eqs. 9 and 42, one has

$$(60) \quad O_{\nu,A,k,g} \Psi \Psi' = \Theta$$

where

$$(61) \quad \Theta(n) = \sum_{\gamma,h,s} \sum_{\gamma',h',s'} |d_{\gamma,h,s}^n|^2 |f_{\gamma',h',s'}^n|^2 |\gamma, h, s\rangle |\gamma', h', s'\rangle |(\gamma, h, s) O_{\nu,A,k,g}(\gamma', h', s')\rangle.$$

As shown, Θ is not a result sequence in the sense that Ψ'' was. To obtain a result sequence one must take the trace over the two initial states for each element of Θ . This gives a sequence $\mathcal{P}_{\Psi,\Psi}$ of density operators where

$$(62) \quad \mathcal{P}_{\Psi,\Psi}(n) = \sum_{\gamma,h,s} \sum_{\gamma',h',s'} |d_{\gamma,h,s}^n|^2 |f_{\gamma',h',s'}^n|^2 \times \rho |(\gamma, h, s) O_{\nu,A,k,g}(\gamma', h', s')\rangle.$$

Inclusion of these sequences into the definitions presented so far requires expansion of the material to define the Cauchy condition and asymptotic relations for sequences of density operators. Since this has not yet been done, this will be left to future work. Also it is not clear if element definitions of $O_{\nu,S,k,g}$, as is done in Eq. 55, are useful here. In any case, one can proceed without these extensions. Also the main results are not affected by this lack.

3.4. Quantum Representation of Real Numbers. The asymptotic equality relation $=_{\infty,k,g}$ can be used to define equivalence classes of Cauchy sequences. Two sequences Ψ and Ψ' are equivalent if and only if they are asymptotically equal:

$$(63) \quad \Psi \equiv \Psi' \Leftrightarrow \Psi =_{\infty,k,g} \Psi'$$

It is straightforward to show from the properties of $=_{\infty,k,g}$ that \equiv has the right properties for a definition of equivalence.

For each Cauchy sequence Ψ let $[\Psi]$ denote the equivalence class containing Ψ . As might be guessed, the set of all these equivalence classes is a quantum representation of the real numbers. Let $R_{k,g}$ denote the set. The subscripts k, g indicate that the representation depends on both the base k and the gauge or basis choice g .

As has been seen each class $[\Psi]$ contains many \mathcal{F}_k valued sequences and at least one $\mathcal{B}_{k,g}$ valued sequence. From this one concludes that the quantum equivalence classes are larger than the classical equivalence classes but that no new classes are present.

The basic relations and operations can be lifted from sequences to the equivalence classes to define the basic relations and operations for a real number field. Let $Re_{i,R,k,g}$ denote the two relations $=_{R,k,g}$ for $i = 1$ and $<_{R,k,g}$ for $i = 2$. Let $[\Psi]$ and $[\Psi']$ denote two equivalence classes of Cauchy sequences. Then

$$(64) \quad [\Psi] Re_{i,R,k,g} [\Psi'] \Leftrightarrow \Psi Re_{i,\infty,k,g} \Psi'.$$

This definition holds for all \mathcal{F}_k valued sequences.

The field operations, $O_{\nu,R,k,g}$ for $\nu = 1 - 4$ ($+, \times, -, \div$), can be defined on equivalence classes through their definitions on $\mathcal{B}_{k,g}$ valued sequences. Let Ψ, Ψ', Ψ'' be Cauchy sequences that satisfy Eqs. 54 and 57. Define $O_{\nu,R,k,g}$ by

$$(65) \quad [\Psi] O_{\nu,R,k,g} [\Psi'] = [\Psi''].$$

This use of $\mathcal{B}_{k,g}$ valued sequences to define the field operations definition is done only because Cauchy sequences of density operators are not included here. Their inclusion would allow direct definitions of the field operators for all Cauchy sequences.

To verify that $R_{k,g}$ is a representation of the real numbers, one must show that $R_{k,g}$ and the relations, $Re_{i,R,k,g}$, and operations $O_{\nu,R,k,g}$, satisfy the real number axioms of a complete ordered field [25]. Some details of this were given in [6], so it will not be repeated here. The proof is, in many ways, similar to that given for the usual classical Cauchy sequences of rational numbers [26].

4. Space of Real Number Representations and Associated Transformations

As described, the quantum theory representations of real numbers, $R_{k,g}$, depend on a base k and a gauge g . Recall that k denotes the dimensionality of the Hilbert space of states for each single q_k and g denotes a gauge field of basis sets on $I \times I$, Eq. 12.

For each pair k, g one has a quantum representation $R_{k,g}$ of the real numbers. Any pair, $R_{k,g}, R_{k',g'}$ of real number representations are isomorphic as all representations of the real numbers (axiomatized by second order axioms) are isomorphic [35]. However this does not mean that they are identical. For instance, Cauchy sequences of q_k string states, which are elements of the equivalence classes in $R_{k,g}$, are distinct from Cauchy sequences of $q_{k'}$ string states, which are elements of equivalence classes in $R_{k',g'}$, as q_k and $q_{k'}$ systems are different.

Similarly $\mathcal{B}_{k,g}$ valued sequences Ψ of q_k string states are different from $\mathcal{B}_{k',g'}$ valued sequences. Also the definition of the Cauchy condition, Eq. 34 is both k and g dependent. These dependencies can be seen from Eqs. 13-16 which show the relations between the two basis sets and between the single q_k A-C operators for each of the two basis sets.

These considerations show that the set of all representations $R_{k,g}$ can be regarded as a space of representations parameterized by a two dimensional space of all pairs, k, g . Transformations $k, g \rightarrow k', g'$ induce transformations $R_{k,g} \rightarrow R_{k',g'}$ on the representation space. The components of the transformations on the representation space are operators that change bases, $R_{k,g} \rightarrow R_{k',g}$, and operators that change the gauge, $R_{k,g} \rightarrow R_{k,g'}$.

4.1. Gauge Changing Operators. Gauge changing operators that act on sequences can be defined from the gauge transformations, U_k as defined in Eqs. 13 and Eq. 14. To achieve this, let Ψ and Ψ' be respective $\mathcal{B}_{k,g}$ and $\mathcal{B}_{k',g'}$ valued sequences where

$$(66) \quad \begin{aligned} \Psi(n) &= |\gamma_n, h_n, s_n\rangle_{k,g} \\ \Psi'(n) &= |\gamma_n, h_n, s_n\rangle_{k',g'}. \end{aligned}$$

Define the operator, \mathcal{U}_k , by

$$(67) \quad \Psi' = \mathcal{U}_k \Psi$$

where

$$(68) \quad |\gamma_n, h_n, s_n\rangle_{k',g'} = U_k |\gamma_n, h_n, s_n\rangle_{k,g}.$$

Here g and g' are related by

$$(69) \quad g' = U_k g.$$

This shows that the elements of $\Psi', \Psi'(n)$, are the same states, relative to the transformed basis as the elements $\Psi(n)$, of Ψ are, relative to the original basis. However, relative to the original basis, the states $\Psi'(n)$ are different from the states $\Psi(n)$. This can be seen by expanding the states $\Psi'(n)$ in terms of the original basis.

The definition of \mathcal{U}_k extends by linearity to \mathcal{F}_k valued sequences. If Ψ is such a sequence where

$$(70) \quad \Psi(n) = \sum_{\gamma, h, s} d_{\gamma, h, s}^n |\gamma, h, s\rangle_{k, g},$$

then Ψ' is related to Ψ by Eq. 67 where

$$(71) \quad \Psi'(n) = \sum_{\gamma, h, s} d_{\gamma, h, s}^n |\gamma, h, s\rangle_{k, g'}$$

Note the replacement of g by g' on the right hand side.

The definition of \mathcal{U}_k can be lifted to apply to equivalence classes of Cauchy sequences to relate $R_{k, g}$ to $R_{k, g'}$ as in $R_{k, g'} = \mathcal{U}_k R_{k, g}$. The validity of this depends on the preservation of the Cauchy property under the action of U_k . That is, if Ψ is a g -Cauchy sequence, then $\Psi' = \mathcal{U}_k \Psi$ is a g' -Cauchy sequence.¹⁰ To show that this is the case one has to define the g' -Cauchy condition relative to the basis states in $\mathcal{B}_{k, g}$. This is

$$(72) \quad \forall \ell \exists p \forall j, m > p (|U_k(\gamma_j, h_j, s_j) -_{A, k, g'} U_k(\gamma_m, h_m, s_m)|_{A, k, g'})_{k, g'} \leq_{A, k, g'} U_k|+, -\ell\rangle_{k, g}.$$

Here $U_k|\gamma_j, h_j, s_j\rangle_{k, g} = |\gamma_j, h_j, s_j\rangle_{k, g'}$, $\leq_{A, k, g'} = U_k \leq_{A, k, g} U_k^\dagger$, and $-_{A, k, g'} = U_k \times U_k \times U_k -_{A, k, g} U_k^\dagger \times U_k^\dagger$. It is a straightforward exercise to show that, for this definition, the Cauchy property is preserved under the action of U_k .

The definition of \mathcal{U}_k shows that these operators form a group of transformations. If \mathcal{U}_k and \mathcal{U}'_k are gauge transformations, for Cauchy sequences, or for equivalence classes in $R_{k, g}$, then so is their product $\mathcal{U}_k \mathcal{U}'_k$. Also each \mathcal{U}_k has an inverse \mathcal{U}_k^{-1} . The group property follows from the fact that the U_k , on which the \mathcal{U}_k are based, are products of elements of the unitary group $U(k)$.

4.2. Base Changing Operators. One would like to describe the base changing transformations for Cauchy sequences by lifting the base changing transformations $\tilde{W}_{k', k}$ for the q_k string states to transformations on the Cauchy sequences. One first thinks of doing this by defining an operator $\mathcal{W}_{k', k}$ on $\mathcal{B}_{k, g}$ valued sequences Ψ . One would set

$$(73) \quad \Psi' = \mathcal{W}_{k', k} \Psi.$$

Here Ψ' is a $\mathcal{B}_{k', g}$ valued sequence such that for each n

$$(74) \quad \Psi'(n) = |\gamma_n, h_n, s'_n\rangle_{k', g} = \tilde{W}_{k', k} |\gamma_n, h_n, s_n\rangle_{k, g} = \tilde{W}_{k', k} \Psi(n)$$

The problem with this definition is that the domain and range of $\tilde{W}_{k', k}$ depend on the relation of the prime factors of k and k' . If k and k' are relatively prime, then this definition fails as $\tilde{W}_{k', k}$ is not defined on any of the non integer states.

One way around this impasse is to generalize the definition of $\tilde{W}_{k', k}$ to operators $\tilde{W}_{k', k, \ell}$ for different nonnegative integers ℓ . Here

$$(75) \quad |\gamma_n, h_n, s'_n\rangle_{k', g} = \tilde{W}_{k', k, \ell} |\gamma_n, h_n, s_n\rangle_{k, g}$$

¹⁰The g' -Cauchy condition is given by Eq. 34 with the subscript g' replacing g .

is a base k' state that represents the same number as the base k state $|\gamma_n, h_n, s_n\rangle_{k,g}$ up to accuracy $|+, -\ell\rangle_{k',g}$. This removes the problem because, for each ℓ , $\tilde{W}_{k',k,\ell}$ is defined on all q_k string states in \mathcal{F}_k . Also $\tilde{W}_{k',k,\ell} = \tilde{W}_{k',k}$ on the integer state subspace of \mathcal{F}_k .

The desired definition of $\mathcal{W}_{k',k}$ is that it be an isomorphism from $R_{k,g}$ to $R_{k',g}$. This is equivalent to requiring that $\mathcal{W}_{k',k}\Psi$ belongs to the equivalence class in $R_{k',g}$ that represents the same number as the equivalence class in $R_{k,g}$ that contains Ψ . A proposed method of achieving this is by a definition that is diagonal in n and in ℓ .

To this end one defines $\mathcal{W}_{k',k}$ by replacing $\tilde{W}_{k',k}$ with $\tilde{W}_{k',k,n}$ in Eq. 74 to get

$$(76) \quad \Psi'(n) = |\gamma_n, h_n, s'_n\rangle_{k',g} = \tilde{W}_{k',k,n}|\gamma_n, h_n, s_n\rangle_{k,g} = \tilde{W}_{k',k,n}\Psi(n).$$

The operator $\mathcal{W}_{k',k}$ must satisfy two properties: The sequence $\Psi = \mathcal{W}_{k',k}\Psi$ must be Cauchy if Ψ is Cauchy, and the two sequences, Ψ' in $R_{k',g}$ and Ψ in $R_{k,g}$, must represent the same real number. (Here and in the following, Cauchy sequences will often be stand ins for equivalence classes of the sequences.) An equivalent requirement is that $\mathcal{W}_{k',k}$ is an isomorphism from $R_{k,g}$ to $R_{k',g}$. It preserves the basic field relations of equality and ordering and the operations of addition, multiplication and their inverses.

5. Quantum Representations of Complex Numbers

The simplest path to descriptions of quantum representations of complex numbers is their representation as ordered pairs of real number representations. If $[\Psi]$ and $[\Psi']$ represent two quantum real numbers, then $([\Psi], [\Psi'])$ represents a quantum complex number where $[\Psi] = [\Psi]^r$ and $[\Psi'] = [\Psi]^i$ represent the real and imaginary components. The basic field relations $=_{R,k,g}, <_{R,k,g}$ and operations $+_{R,k,g}, \times_{R,k,g}, -_{R,k,g}, \div_{R,k,g}$ would be extended to relations $=_{C,k,g}, <_{C,k,g}$ and operations $+_{C,k,g}, \times_{C,k,g}, -_{C,k,g}, \div_{C,k,g}$ following the standard rules.

The rest of this section can be skipped over by readers using the above definitions. The following development is based on the observation that all physical representations of complex numbers, such as in computations, are by ordered pairs of single string representations of rational numbers. This corresponds here to extending the treatment of rational number representations, as states of q_k strings, to ordered pairs of states of q_k strings. These represent the real and imaginary components of complex rational numbers. Application of the Cauchy condition separately to the real and imaginary components gives a description of Cauchy sequences of complex rational number representations. This gives quantum representations of complex numbers as equivalence classes of these Cauchy sequences.

One way to proceed is to continue working with one type of qubit but increase the number of sign qubit types from one to two.¹¹ The two qubit types are represented by A-C operators $c_{\gamma,0,h}^\dagger, d_{\delta,0,h}^\dagger$ and their complex conjugates. Here $c_{\gamma,0,h}^\dagger$ and $d_{\delta,0,h}^\dagger$ represent sign creation operators for the real and imaginary number components where $\gamma = +, -$ and $\delta = +i, -i$ at site $0, h'$

¹¹This differs from the approach in [6] which uses two types of qukits and qubits.

Complex rational numbers are represented here by pairs of qukit string states, $|h, \gamma, s; h', \delta, t\rangle_{k,g}$, with different h values. In terms of A-C operators one has

$$(77) \quad |h, \gamma, s; h_1, \delta, t\rangle_{k,g} = c_{\gamma,0,h}^\dagger (a^\dagger)_{[(l,h),(u,h)]}^s; d_{\delta,0,h_1}^\dagger (a^\dagger)_{[(l',h_1),(u',h_1)]}^t |0\rangle.$$

The state $|0\rangle$ denotes the qukit vacuum and $0, h$ and $0, h_1$ denote the locations of the sign qubits. As before $[(l, h), (u, h)]$ and $[(l', h_1), (u', h_1)]$ denote lattice intervals where $l \leq 0 \leq u$ and $l' \leq 0 \leq u'$. Also

$$(78) \quad \begin{aligned} (a^\dagger)_{[(l,h),(u,h)]}^s &= a_{s(u),u,h}^\dagger a_{s(u-1),u-1,h}^\dagger \cdots a_{s(l),l,h}^\dagger \\ (a^\dagger)_{[(l',h_1),(u',h_1)]}^t &= a_{t(u'),u',h_1}^\dagger a_{t(u'-1),u'-1,h_1}^\dagger \cdots a_{t(l'),(l',h_1)}^\dagger \end{aligned}$$

where s and t are $0, \dots, k-1$ valued functions with integer interval domains $[l, u]$ and $[l', u']$ respectively. The subscript g denotes the implicit gauge choice for the q_k^r string states at each site of $I \times I$.

A consequence of this representation is that if one has many pairs of string states, they are expressed in the A-C formalism as one long string of creation operators acting on $|0\rangle$. One then needs a method of determining the association between the imaginary and real strings. One of the different ways to do this is to describe the pairs as those in which h is close or next to h_1 . Here some method will be assumed implicitly as which one is used does not affect the results obtained in this paper.

The definitions of arithmetic relations and operations given for states of q_k strings can be easily extended to states of pairs of q_k strings following the usual arithmetic rules for operations on complex numbers. For arithmetic equality one has

$$(79) \quad \begin{aligned} |h, \gamma, s; h_1, \gamma_1, t\rangle_{k,g} &=_{c,k,g} |h', \gamma', s', h'_1, \gamma'_1, t'\rangle_{k,g} \\ \Leftrightarrow (|h, \gamma, s\rangle_{k,g} &=_{r,k,g} |h', \gamma', s'\rangle_{k,g} \\ \text{and } |h_1, \gamma_1, t\rangle_{k,g} &=_{i,k,g} |h'_1, \gamma'_1, t'\rangle_{k,g}). \end{aligned}$$

Ordering relations are usually not considered because they are only partly defined (complex numbers cannot be ordered). The c, r, i in the subscripts denote complex, real, and imaginary, respectively.

For the operations let $\tilde{O}_{c,k,g}$ be a unitary operator denoting any of the four operations $+_{c,k,g}, \times_{c,k,g}, -_{c,k,g}, \div_{c,k,g,\ell}$. The action of any of these on complex rational states can be represented by

$$(80) \quad \begin{aligned} \tilde{O}_{c,k,g} |h, \gamma, s; h_1, \delta, t\rangle_{k,g} |h', \gamma', s'; h'_1, \delta', t'\rangle_{k,g} \\ = |h, \gamma, s; h_1, \delta, t\rangle_{k,g} |h', \gamma', s'; h'_1, \delta', t'\rangle_{k,g} |h'', \gamma'', s''; h''_1, \delta'', t''\rangle_{k,g} \end{aligned}$$

where

$$(81) \quad |h'', \gamma'', s''; h''_1, \delta'', t''\rangle_{k,g} =_{c,k,g} |(h, \gamma, s; h_1, \delta, t) O_{c,k,g} (h', \gamma', s'; h'_1, \delta', t')\rangle_{k,g}.$$

The expression $|(h, \gamma, s; h_1, \delta, t) O_{c,k,g} (h', \gamma', s'; h'_1, \delta', t')\rangle_{k,g}$ with O inside $|-,-\rangle$ represents the rational string state resulting from carrying out the operation $O_{c,k,g}$. Unitarity is satisfied by preserving the two input states and creating a result state.

The arithmetic operations create entangled states when applied to linear superpositions of the basis states. One has

$$(82) \quad \begin{aligned} \tilde{O}_{c,k,g}\psi\psi' &= \sum_{h,\gamma,s,h_1,\delta,t} \sum_{h',\gamma',s',h'_1,\delta',t'} k, g \langle h, \gamma, s; h_1, \delta, t | \psi \rangle \\ &\times k, g \langle h', \gamma', s'; h'_1, \delta', t' | \psi' \rangle |h, \gamma, s; h_1, \delta, t\rangle_{k,g} |h', \gamma', s'; h'_1, \delta', t'\rangle_{k,g} \\ &\times |(h, \gamma, s; h_1, \delta, t) O_{c,k,g}(h', \gamma', s'; h'_1, \delta', t')\rangle_{k,g}. \end{aligned}$$

Taking the trace over the ψ and ψ' component states gives a mixed state

$$(83) \quad \begin{aligned} \rho_{\psi O_{c,k,g}\psi'} &= \sum_{h,\gamma,s,h_1,\delta,t} \sum_{h',\gamma',s',h'_1,\delta',t'} |\langle h, \gamma, s; h_1, \delta, t | \psi \rangle|^2 \\ &\times |\langle h', \gamma', s'; h'_1, \delta', t' | \psi' \rangle|^2 \rho_{(h,\gamma,s;h_1,\delta,t) O_{c,k,g}(h',\gamma',s';h'_1,\delta',t')} \end{aligned}$$

that represents the result of the operation.

Determination of the exact form of the state $|h'', \gamma'', s''; h''_1, \delta'', t''\rangle_{k,g}$ from Eq. 81 for the different arithmetic operations is somewhat lengthy, but straightforward. It involves translation of the usual rules for implementation of arithmetic operations on complex numbers into those on quantum states. For example, for multiplication one uses the relations

$$(84) \quad \begin{aligned} d_{\gamma,0,h}^\dagger \times d_{\gamma',0,h'}^\dagger &= c_{\gamma'',0,h''}^\dagger \text{ where } \gamma'' = +, [-] \text{ if } \gamma \neq [\neq] \gamma' \\ c_{\gamma,0,h}^\dagger \times d_{\gamma',0,h'}^\dagger &= d_{\gamma'',0,h''}^\dagger \text{ where } \gamma'' = \gamma', [\gamma' \neq \gamma''] \text{ if } \gamma = +[\gamma = -] \\ c_{\gamma,0,h}^\dagger \times c_{\gamma',0,h'}^\dagger &= c_{\gamma'',0,h''}^\dagger \text{ where } \gamma'' = +, [-] \text{ if } \gamma = \gamma'[\gamma \neq \gamma']. \end{aligned}$$

Quantum representations of complex numbers are based on application of the Cauchy condition to the real and imaginary components separately of a sequence of states of q_k string pairs. The sequence Ψ where $\Psi(n) = |h_n, \gamma_n, s_n; h'_n, \delta_n, t_n\rangle_{k,g}$ of states is a Cauchy sequence if the following is satisfied:

$$(85) \quad \begin{aligned} \forall \ell \exists p \forall j, m > p & | |(h_j, \gamma_j, s_j) -_{r,k,g} (h_m, \gamma_m, s_m)|_{r,k,g} \rangle_{k,g} <_{r,k,g} |+, -\ell\rangle_{k,g} \\ \text{and } | |(h'_j, \delta_j, t_j) -_{i,k,g} (h'_m, \delta_m, t_m)|_{i,k,g} \rangle_{k,g} &<_{r,k,g} |+, -\ell\rangle_{k,g}. \end{aligned}$$

Here $|+, -\ell\rangle_{k,g}$ is the state corresponding to the number $k^{-\ell}$.

Extension of the Cauchy condition to sequences of linear superpositions of complex rational string states is similar to that for sequences of superpositions of real rational states. Such a sequence is Cauchy if the probability is unity that both the real and imaginary components satisfy the Cauchy condition.

The definition of equivalence for the real number representations extends here to complex number representations. Two Cauchy sequences Ψ and Ψ' are equivalent if the real and imaginary components of Ψ and Ψ' are asymptotically equal. Let Ψ and Ψ' be $\mathcal{B}_{k,g}$ valued sequences where for each n

$$(86) \quad \begin{aligned} \Psi(n) &= |h_n, \gamma_n, s_n; h_{1,n}, \delta_n, t_n\rangle_{k,g} \\ \Psi'(n) &= |h'_n, \gamma'_n, s'_n; h'_{1,n}, \delta'_n, t'_n\rangle_{k,g}. \end{aligned}$$

Then

$$(87) \quad \begin{aligned} \Psi =_{\infty,S,k,g} \Psi' & \text{ if } \forall \ell \exists p \forall j, m > p \\ & | |(h_j, \gamma_j, s_j) -_{r,k,g} (h'_m, \gamma'_m, s'_m)|_{r,k,g} \rangle_{k,g} \leq_{r,k,g} |+, -\ell\rangle_{k,g} \text{ and} \\ & | |(h_{1,j}, \delta_j, t_j) -_{i,k,g} (h'_{1,m}, \delta'_m, t'_m)|_{i,k,g} \rangle_{k,g} \leq_{r,k,g} |+, -\ell\rangle_{k,g}. \end{aligned}$$

From this definition one has¹²

$$(88) \quad \Psi \equiv \Psi' \text{ if } \Psi =_{\infty, S, k, g} \Psi'.$$

The set $C_{k, g}$ of complex numbers is defined to be the set of equivalence classes $[\Psi]$ where Ψ is a Cauchy sequence of $q_2^r q_k, q_2^i q_k$ string pairs. Here q_2^r and q_2^i denote the real and imaginary sign qubits. As was the case for $R_{k, g}$, each equivalence class is larger than the corresponding classical equivalence class, but there are no new equivalence classes. This follows from the observation that each class contains at least one $\mathcal{B}_{k, g}$ valued sequence.

The basic field relation $=_{C, k, g}$ is defined by

$$(89) \quad [\Psi] =_{C, k, g} [\Psi'] \text{ if } \Psi =_{\infty, S, k, g} \Psi'$$

The operations $\tilde{+}_{C, k, g}, \tilde{-}_{C, k, g}, \tilde{\times}_{C, k, g}, \tilde{\div}_{C, k, g}$, are defined in a similar fashion. For $\mathcal{B}_{k, g}$ valued Cauchy sequences one has expressions similar to Eqs. 54 et seq:

$$(90) \quad \tilde{O}_{\nu, C, k, g}[\Psi][\Psi'] = [\Psi][\Psi'][\Psi'']$$

Here $\tilde{O}_{\nu, C, k, g}$ with $\nu = 1, 2, 3, 4$ is a stand in for the four operations. For $\nu = 1, 2, 3$ the class $[\Psi'']$ contains all Cauchy sequences asymptotically equal to Ψ'' where

$$(91) \quad \Psi''(n) = |\Psi(n) O_{\nu, c, k, g} \Psi'(n)\rangle_{k, g}.$$

For $\nu = 4$, $(\div_{C, k, g})$ one has a diagonal definition similar to Eq. 59¹³:

$$(92) \quad \Psi''(n) = |\Psi(n) \div_{c, k, g, n} \Psi'(n)\rangle_{k, g}.$$

As is the case for real number representations, these relations and operations extend to \mathcal{F}_k valued Cauchy sequences. Details will not be given here as they are an extension of those for the real number representations.

6. Fields of Quantum Reference Frames

At this point it is good to step back and view some consequences of the existence of the many different representations of R and C . All physical theories considered to date, and many mathematical theories, can be regarded as theories that are based on the real and complex numbers. Included are quantum and classical mechanics, quantum field theory, QED, QCD, special and general relativity, and string theory. It follows that for each representation $R_{k, g}, C_{k, g}$ of R and C one has a corresponding representation of physical theories as mathematical structures based on $R_{k, g}, C_{k, g}$

¹²It is easy to see that this definition of \equiv has the necessary properties of symmetry, reflexivity, and transitivity. These follow from the corresponding properties of $=_{\infty, S, k, g}$.

¹³The specific definitions of these operations follows those for complex numbers. As examples, for multiplication, if $\Psi(n) = |h_n, \gamma_n, s_n; h_{1, n}, \delta_n, t_n\rangle_{k, g} = |x, iy\rangle$ and $\Psi'(n) = |h'_n, \gamma'_n, s'_n; h'_{1, n}, \delta'_n, t'_n\rangle_{k, g} = |x', iy'\rangle$, then

$$\Psi''(n) = |(x \times_{r, k, g} x') -_{r, k, g} (y \times_{i, k, g} y'); \\ (x \times_{i, k, g} y') +_{i, k, g} (x' \times_{i, k, g} y)\rangle_{k, g}.$$

Division to accuracy n of $|x, y\rangle$ by $|x', y'\rangle$ is done by carrying out the division to accuracy n indicated by

$$|x'', y''\rangle = |[Re, Im] \div_{c, k, g, n} (x' \times x') + (y' \times y')\rangle$$

where $Re = x \times x' + y \times y'$ and $Im = x' \times y - x \times y'$.

The large number of theories based on R, C suggests that one associate a reference frame $F_{k,g}$ with each R, C representation, $R_{k,g}, C_{k,g}$. Here $R_{k,g}, C_{k,g}$ is referred to as the base of frame $F_{k,g}$. The frame $F_{k,g}$ contains representations of all physical theories that are representable as structures based on $R_{k,g}, C_{k,g}$.

The large number of real and complex number representations and associated reference frames suggests that one define a frame field F over the two dimensional parameter space $\{k, g\}$. The components of F , as a map from $\{k, g\}$ to a set of reference frames, are the frames $F_{k,g}$ at each value k, g . Note that the parameter g is unique to quantum theory representations as it is not applicable to representations based on states of classical kit strings. However, the parameter k is common to both qukit and kit string representations.

This construction is shown schematically in Figure 1 for three of the infinite number of values of k, g . This is shown by solid arrows coming from the parent frame $F_{R,C}$ to three of the infinitely many descendent frames.

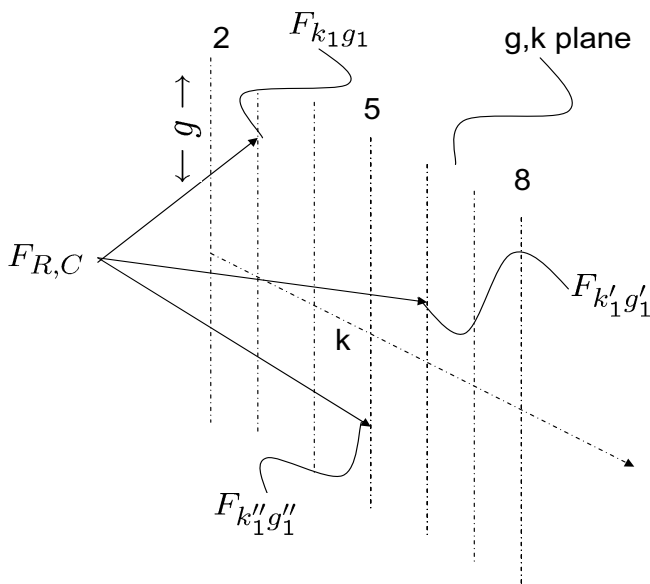


FIGURE 1. Schematic illustration of frames coming from frame $F_{R,C}$. The frames are based on quantum representations of real and complex numbers in $F_{R,C}$. The distinct vertical lines in the k, g plane denote the discreteness of the integral values of $k \geq 2$. Only three of the infinitely many frames coming from $F_{R,C}$ are shown. Here k denotes the qukit base and g denotes a gauge or basis choice.

This use of reference frames has much in common with other uses of reference frames in physics and particularly in quantum theory [27, 28, 30, 31, 32, 33]. In special relativity, inertial coordinate systems define reference frames for describing physical dynamics. In quantum cryptography, Alice and Bob pick a polarization direction to define a reference frame for sending messages encoded in qubit string

states. Here each reference frame carries representations of all physical theories as mathematical structures based on the real and complex number base of the frame.

It is of interest to examine what observers can and cannot see in the different frames. To begin it is assumed that an observer O_R in the parent frame $F_{R,C}$ regards the real and complex numbers in the frame base as elementary objects. The only relevant properties they have are those required by the relevant axioms for R and C ¹⁴. This assumption is based on the prevalent view taken by physics so far of the nature of real and complex numbers, that they are elementary objects. The only properties of these objects that physics cares about are those derivable from the relevant axioms.

The quantum theory representations of real and complex numbers described here suggest that O_R sees that $R_{k,g}$ and $C_{k,g}$, as equivalence classes of Cauchy sequence of states of q_k strings, represent real and complex numbers. O_R also sees that $R_{k,g}$ and $C_{k,g}$, can serve as the base of a frame $F_{k,g}$ containing representations of physical theories as mathematical structures based on $R_{k,g}, C_{k,g}$.

Symmetry considerations suggest that an observer $O_{k,g}$ in each frame, $F_{k,g}$, has the same view relative to $F_{k,g}$ as O_R does relative to the frame $F_{R,C}$. Thus $O_{k,g}$ sees $R_{k,g}, C_{k,g}$ as elementary, structures whose only relevant properties are those derivable from the relevant axiom sets. The structure of the elements of $R_{k,g}, C_{k,g}$, as equivalence classes of Cauchy sequences, seen by O_R , are not visible to $O_{k,g}$. Also the construction, in $F_{R,C}$, of representations, $R_{k,g}, C_{k,g}$, can be repeated in $F_{k,g}$ to obtain representations $R_{2,k',g'}, C_{2,k',g'}$. Here 2 is the iteration stage. This is visible to an observer $O_{k,g}$ in $F_{k,g}$. The construction in $F_{k,g}$ is possible because $F_{k,g}$ contains representations of physical theories, including quantum theory, as structures based on $R_{k,g}, C_{k,g}$.

It follows that this construction can be iterated to obtain frames emanating from frames. The iteration or stage number provides a third dimension to the frame field where for each number j , $F_{j,k,g}$ denotes a frame at stage j .

There are several different iteration types to consider: a finite number of iterations, a one way infinite number, a two way infinite number, and a finite cyclic iteration. All these types are mathematically possible. They must all be considered as there is no a priori reason to choose one type over another. The different types are illustrated schematically in figures 2 -4.

Figure 2 shows the frame field for a finite number, n , of iterations. The iteration paths shown represent two out of an infinite number of paths. Each path segment, shown by an arrow, stands for a quantum theory representation of real and complex numbers described in the frame at the arrow tail. The frame at the arrow head is based on the described quantum theory representation. The iteration direction is shown by the arrows.

Figs. 1 and 2 show the existence of a fixed frame which is an ancestor for all the frames in the field. This is the case even if n is extended to infinity in Fig. 2 to give a one way infinite iteration. Here, too, there is a fixed elementary representation of the real and complex numbers that is external to the whole field.

¹⁴The axioms for real and complex numbers are respectively those describing a complete, ordered field [36] and an algebraically closed field of characteristic 0 [37].

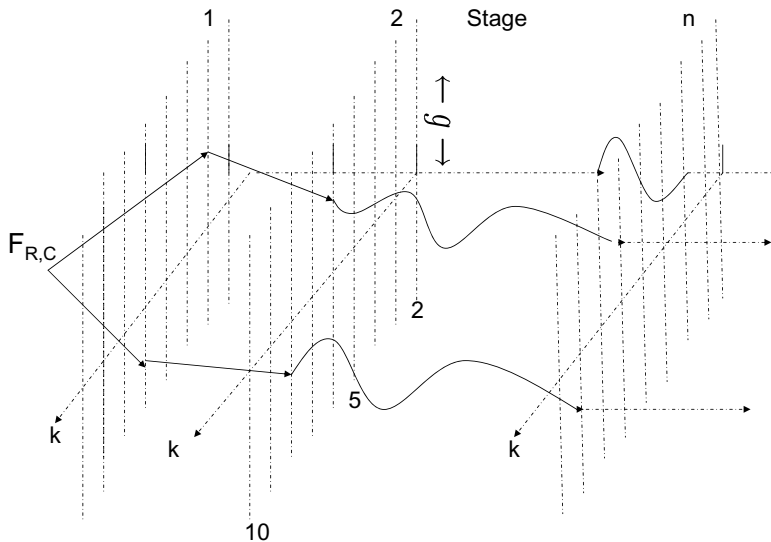


FIGURE 2. Schematic illustration of a finite number n of frame generations coming from frame $F_{R,C}$. The stage number is given at the top. The direction of the iterations are shown by the solid connected arrows showing sample iteration paths from $F_{R,C}$ through the k, g planes and ending at the n th plane. The horizontal dashed lines at the right end indicate that in the case of a one-way infinite number of iterations there is no terminal stage n for any finite n . See Fig. 1 caption for more details.

The two way infinite and cyclic iterations shown in Figs. 3 and 4 are different in this respect. There is no representation of the real and complex numbers that is external for the whole frame field. All are inside some frame as each frame has parent frames. There is no common ancestor frame.

The path shown in Figure 4 for cyclic iterations is an example of a path with winding number 1 in that it comes to its starting point in one turn around the iteration cylinder. One can, in principle at least have paths with finite winding numbers or even infinite winding numbers in that they never return to the starting point. One hopes to study in the future these types of paths and their dependence on the number of iterations.

The schematic nature of these figures is to be emphasized. Besides showing that two dimensions of the three dimensional frame field are discrete and one, the gauge dimension, is continuous, they are very useful to show what an observer sees in each frame as well as to illustrate the relation between frames in different generations. They are also illustrations of the different iterations that are mathematically possible. Which of the cases is relevant to physics will have to await more work.

The relations between the observers in different frames, described for Fig. 1, is easily extended to multiple iteration stages shown in the other figures. Observers

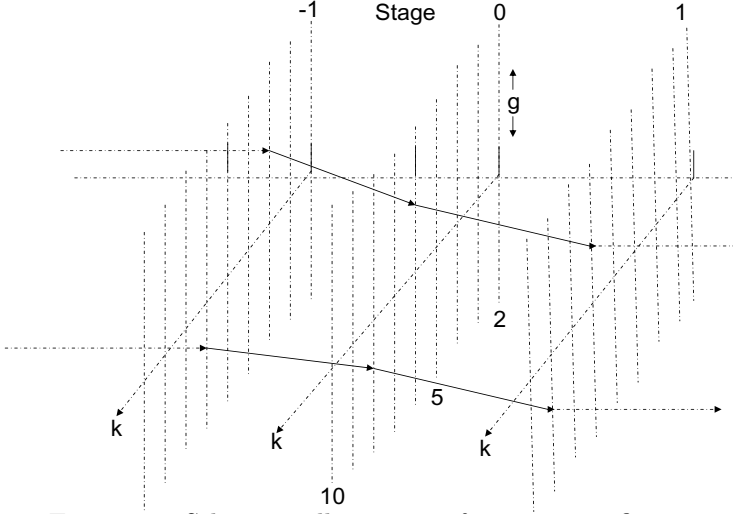


FIGURE 3. Schematic illustration of a two way infinite number of iterations. Here there is no common ancestral frame as all frames have parent frames and descendent frames. The stage number is given at the top. The direction of the iterations are shown by the solid connected arrows showing a possible path from one stage to the next with no beginning or end.

in each frame have in common the property that they can see down the field in the direction of the iterations. That is they can see all their descendent frames, but they cannot see any ancestor frames. They also cannot see any other frame at the same iteration stage. By "see frames and their relations" is meant that an observer $O_{j,k,g}$ in frame $F_{j,k,g}$ can show the presence of the 2 dimensional frame field $F_{j+1} : \{k, g\} \rightarrow \{F_{j+1,k,g}\}$. This is what most of this paper has shown. $O_{j,k,g}$ can also shift the derivation by one or more iteration stages to stage $j+2, j+3$ frames, etc. $O_{j,k,g}$ can also see that the R, C representations in these descendent frames have structure as equivalence classes of Cauchy sequences of (pairs of, for C) finite q_k string states.

However $O_{j,k,g}$ cannot describe either ancestor frames or other stage j frames. Doing so requires awareness of the real and complex number base of a parent frame. These are not available as they are outside of $F_{j,k,g}$.

It is also clear that no observer in a frame can see the whole frame field. This view is reserved for an observer outside the whole field.¹⁵ An observer, $O_{R,C}$, in a common ancestral frame $F_{R,C}$ can see the whole descendent frame field structure. However $O_{R,C}$ cannot tell if there are one or more ancestor stages above.

¹⁵Here it is assumed that any reader of this paper is outside the whole frame field. Whether this needs to be revised or not must await further work.

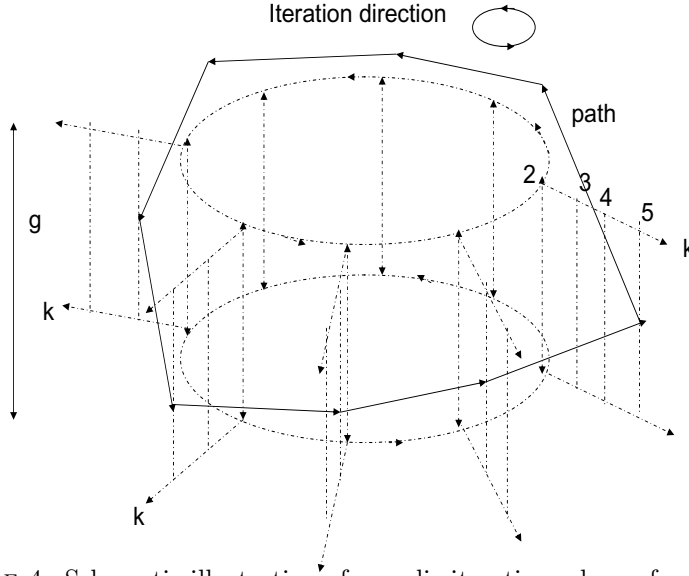


FIGURE 4. Schematic illustration of a cyclic iteration scheme for a finite number (8) of iterations. There is no common ancestral frame as all frames have parent frames and descendent frames. The stage number is given at the top. The direction of the iterations are shown by the solid connected arrows showing a possible cyclic path. To avoid clutter, the three g, k planes in the back have been suppressed.

In many ways this is like the bird (outside the system) and frog (inside the system) views used [8, 9] by Tegmark¹⁶ In effect one has here a hierarchy of bird and frog views. An observer, $O_{j,k,g}$, in a frame, $F_{j,k,g}$ has a frog view of $F_{j,k,g}$ and of the theories in $F_{j,k,g}$. $O_{j,k,g}$ sees the real and complex number base, $R_{j,k,g}$, $C_{j,k,g}$ as elementary. The only relevant properties they have are those derived from the relevant set of axioms. However, $O_{j,k,g}$ has a birds view of all descendent frames in that the relations between all descendent frames are visible.

Cyclic frame iterations present a different situation in that descendant frames are also ancestor frames. Because of this one may have to relax the stipulation that an observer cannot see an ancestor frame. Details of exactly how this would occur are not known at present.

The iteration paths illustrated in the figures give a good representation of what observers in different frames can and cannot see. Each path is a "visibility" path for each frame on the path. If $F_{j,k,g}$ is on a path, then any frame $F_{j',k',g'}$ with $j' > j$ on the path is a descendent frame and is visible from $F_{j,k,g}$. Frames $F_{j',k',g'}$ with $j' < j$ are not visible from $F_{j,k,g}$ (except possibly in the cyclic case).

¹⁶These concepts also play a role in mathematical logic in discussions of "absoluteness", i.e. whether or not properties of systems in a model of a set of axioms are preserved when one moves from a view inside the model to one outside the model.[38]

The totality of frame visibility from $F_{j,k,g}$ is then given by the descendant frames in all paths passing through $F_{j,k,g}$.

The presence of a three dimensional frame field shows that quantum theory representations have two additional dimensions for the frame field that are not present in classical representations based on kit strings. One is the presence of the freedom of gauge or basis choice. The other is based on the fact that quantum theory, in common with other physical theories, is a theory based on the real and complex numbers. The relevant point here is that states of finite strings of qukits are elements of a Fock space which is itself based on the real and complex numbers. This also applies to the states of individual q_k which are elements of a k dimensional Hilbert space. Both these spaces are vector spaces over the complex field C .

7. Integration with Physics

The main problem confronting this work is how to integrate quantum representations of real and complex numbers and fields of iterated reference frames with physics. This relationship would be expected to be an important part of any approach to a coherent theory of physics and mathematics [4, 5], or to any general theory in which physical and mathematical systems are closely related [8]. In particular one may hope that elucidation of this relationship will provide a good foundation to theoretical physics. It also may help to decide which of the different competing theories of quantum gravity, such as loop quantum gravity [40] and string theory [41], is correct.

7.1. Simple Relations to Physics. There are some simple ways the work presented here is related to physics. They are called simple only because it is not clear if they would influence the properties of physical theories or affect physics.

One of these, which was noted earlier, is that the choice of number representations as states of single finite q_k strings is based on the universality of quantum mechanics as a description of physical systems. Also influencing the choice is the fact that all physical representations of numbers are as states of finite strings of physical systems.

The important role that real and complex numbers have in physics should also be stressed. All theoretical predictions of physical properties of systems are in the form of real numbers as values of physical properties. Also dimensionless constants are presumed to be real numbers. Complex numbers occur as expansion coefficients of superposition states of physical systems and as elements in matrix representations of operators.

Translation of this into the frame field described here has consequences of how the numbers used by physical theories in a frame are seen by observers in different frames. For example an observer $O_{j,k,g}$ in frame $F_{j,k,g}$ sees the real and complex numbers, $R_{j,k,g}, C_{j,k,g}$, as external featureless objects with no properties other than those derived from the real and complex number axioms. Any other properties they may have are not visible to $O_{j,k,g}$.

It follows that, from $O'_{j,k,g}$'s viewpoint, all values of physical quantities described or predicted by physical theory representations, as mathematical structures based on $R_{j,k,g}, C_{j,k,g}$ have the same property to $O_{j,k,g}$. This applies to both dimensionless physical quantities such as the fine structure constant and dimensioned quantities such as values of spatial position, distance, momentum, energy, all elements of the spectrum of observables, values of the metric tensor $g_{\mu,\nu}$, etc.

However an observer $O_{j',k',g'}$ in a parent frame $F_{j',k',g'}$ where $j' = j - 1$ sees all elements of $R_{j,k,g}$ as equivalence classes of states of finite q_k strings. As a result $O_{j',k',g'}$ also sees that all physical quantities described by theories in $F_{j,k,g}$ are equivalence classes of Cauchy sequences of q_k string states. To summarize, what $O_{j,k,g}$ sees as elementary featureless objects, are seen by $O_{j',k',g'}$ as equivalence classes of Cauchy sequences of states of q_k strings.

The same holds for representations of all complex valued physical quantities, such as elements of matrices representing physical transformations, and quantum state expansion coefficients. These quantities in frame $F_{j,k,g}$ are seen by $O_{j',k',g'}$ in $F_{j',k',g'}$ as equivalence classes of pairs of qukit string states.

In general, all these results on how the values of physical quantities are seen depends on the relation between the frame containing the representations of these quantities and the viewing frame of an observer. They all follow from the observations that in each frame all physical theories are represented as mathematical structures based on the real and complex number base of the frame. How these numbers are seen depends on the relation between the frame based on these numbers and the viewing frame.

Because of much interest in quantum gravity and associated structure of space and time [39], it is worthwhile to consider how a representation of space time and its properties in one frame are viewed from a parent frame. As would be expected, real number values of all physical properties of space and time, which are featureless and elementary in one frame, are viewed as equivalence classes of Cauchy sequences of states of finite q_k strings from a parent frame. This applies to distances, angles, coordinate positions, and to values of the metric tensor $g_{\mu,\nu}(x)$. It also applies to matrix representations of space time transformations from one inertial frame to another.

In addition, if one regards the points of the space time manifold as 4-tuples, R^4 , of the real numbers, then the same arguments hold. In this case an observer in frame $F_{j,k,g}$ sees the points of his own space time manifold, $R^4_{j,k,g}$ as 4-tuples of elementary, featureless points whereas an observer $O_{j',k',g'}$ in a parent frame $F_{j',k',g'}$ sees the points of $R^4_{j,k,g}$ as 4-tuples of equivalence classes of Cauchy sequences of q_k string states. To $O_{j',k',g'}$ the space time points in $F_{j,k,g}$ are not featureless as they have structure.

This description of how observers describe space time representations in different frames is valid only if one describes the space time manifold as a 4-tuple of real numbers. For other descriptions, such as discrete space times or space time foams [42, 43, 44, 45, 46, 47, 48] or space represented by spin networks [40], it is not clear if a similar description applies that is based on the relation between the viewing and representation frames.

Another aspect of integrating the frame field with physics is that there is no hint of the frame field structure in the properties of the observed physical universe. This suggests that one should perhaps find some way to collapse the field structure, or at least make the different reference frames appear to be "the same" in some sense. This suggests that one should require that the physical properties of systems represented by frame field elements are frame invariant. That is, they are invariant under transformations from one frame to another.

One step in this direction is to require that the field structure be such that all frames are equivalent. This would restrict the iteration types to the two way infinite and finite circular ones as they do not have an ancestor frame that is different (from the viewpoint of outside the frame field) from the other reference frames. It also seems appropriate to restrict consideration to the finite cyclic iteration field type, as one way to move toward frame invariance is to reduce the size of the frame field.

The ultimate step in this direction is to reduce the number of iteration stages in a cycle to just one. Whether this is possible or not will have to await future work.

Another approach to reduce the frame field is to eliminate the gauge dimension entirely by requiring the states of the individual q_k to be invariant under any basis change. This can be achieved by letting the 0 and 1 states of each q_k be represented by different irreducible representations of the gauge group $SU(k)$. One method [31, 49, 50] involves constructing new qukits from the old ones by reducing the product $SU(k) \times SU(k)$ into a sum of irreducible representations and choosing any two representations to represent the 0, 1 states of each new q_k .

Another method [40, 51] uses transformations on the $SU(k)$ group manifold to construct irreducible representations of the group that are invariant under the transformations. In essence this is the method used to construct angular momentum state subspaces labeled by different values of L that are invariant under rotations as transformations on $SO(3)$.

7.2. Speculative Approaches to Integration with Physics. So far the approaches to integrating the frame field and quantum representations of real and complex numbers with physics are rather superficial. They do not represent a real integration that treats both physical and mathematical systems together in a coherent way.

How one does this is quite open at present. However one may speculate about various methods to achieve this. One possible way is based on noting that, as units of quantum information, the qukits be considered to be fundamental objects that can represent either components of numbers or physical systems. Whether it represents a number component (digit) or a physical system would depend on how it is viewed.

The details of this would have to be worked out to see if it has merit. However, it is worth noting that this type of dependence already occurs elsewhere in physics, such as the wave-particle and other types of duality. Also the suggestion that one consider the prime number qukits as elementary and the others as composites, may fit in here. In particular the observation is intriguing that, if the prime numbers p

are related to particle spin by $p = 2s + 1$, there is just one fermion for $s = 1/2$; all the rest are bosons.

Another approach to constructing a coherent integration with physics is based on the observation that physical theory representations have been inserted into each frame of a completed frame field as mathematical structures based on the real and complex number base of the frame. Instead one may consider involving physical theories in the process of constructing Cauchy sequences, their use to represent real and complex numbers, and in properties of the frame field.

In this way physical theories may have input into constructing their real and complex number bases and, conversely, the process of constructing sequences and imposing the Cauchy condition may influence the properties of the physical theories whose base is being constructed. It is even possible that the restrictions imposed by this interlocking process may influence the physical predictions that the theories can make.

It would seem that this approach might be most fruitful in applying it to the cyclic frame fields and possibly those with a very few elements in a cycle. One may speculate that the process of closing the cyclic fields imposes restrictions on the physical theories and numbers involved that influences the values of fundamental constants in the theories or predicted values of physical quantities.

Another approach to integrating this work with physics is based on the possible representation of a sequence Ψ as a $\mathcal{B}_{k,g}$ or, more generally, as an \mathcal{F}_k valued quantum field on the nonnegative integers. Then the states of the field at each n are given by $\Psi(n)$. Attention is then restricted to those fields that satisfy the Cauchy condition, i.e. the Cauchy fields.

As was seen, one of the degrees of freedom in representing these fields is the freedom of gauge or basis choice. Changes in gauge are implemented by gauge transformations acting on the fields as shown in Eq. 67, or $\Psi' = \mathcal{U}_k \Psi$.

This raises the possibility of using the well developed techniques of gauge theories for these fields. For example, one requires that the axioms for the type of numbers being described must be invariant under any gauge transformation. Yet it is clear from their expression in any particular gauge that their expressions transform covariantly under any gauge transformation. The same holds for the expression of the Cauchy condition. This is, ultimately, a consequence of the gauge dependence shown in Eqs. 28 and 27.

One should note that the invariance of the axioms of number theories under gauge transformations also applies to the axioms for any physical theory. The importance of this stems from the fact that all physical theories have axioms, whether they are implicit or explicitly stated. Without axioms, theories are empty as nothing can be derived or predicted.

For the gauge theory approach one can ask if there is any way to express an action or type of LaGrangian whose invariance under gauge transformations expresses the invariance of the axioms for numbers and for physical theories. If so it may be one way to work towards integrating the results obtained here with physics.

There is an intriguing connection of this approach to the standard model in physics [52, 53]. This model is a gauge theory where invariance of the LaGrangian

under gauge transformations requires the introduction of fields for the electromagnetic, weak, and strong forces. The invariance is under all gauge transformations in the group $U(1) \times SU(2) \times SU(3)$.

The connection of the standard model to the gauge theory approach to axiom invariance noted above is based on the earlier suggestion that prime number quikits (those whose base k is a prime number) are elementary and the others are composites. Here invariance is under all gauge transformations in $U(1) \times SU(2) \times SU(3) \times SU(5) \times \dots$. The first three groups in the product are the same as those for the standard model. Whether or not the product of groups $SU(p)$ has to include components for all prime numbers or can be cut off is not known at present.

It is not clear if this, or any other speculative approach, will work out. However, these possibilities indicate that there is much work needed to integrate quantum theory representations of numbers and the resulting frame field with physics.

8. Discussion

There are some other aspects of this work that should be noted. One is that representation of gauge transformations by one continuous dimension of the frame fields, as in Figs. 1-4, is purely schematic. Nothing is implied about what it means for one gauge g to be close to or far away from another. Indeed it may not be useful or even possible to assign a distance measure to the set of gauges.¹⁷

In this connection one should note that the choice of basis sets $\mathcal{B}_{k,g}$ and $\mathcal{B}_{k',g}$ in the spaces \mathcal{F}_k and $\mathcal{F}_{k'}$ is completely arbitrary.¹⁸ There is no way to determine if the g for the $q_{k'}$ strings is the same or different than the g for the q_k strings.

This is different from the usual situation in physics. There one has an external reference field or frame that can be used to define what it means for a basis of k dimensional systems to be the same or different from a basis of k' dimensional systems. Here no such field or common reference frame is present.

In spite of this the two basis sets can be connected by the base changing operator $\tilde{W}_{k',k}$ defined earlier. Recall that if the state $|\gamma, h, s\rangle_{k,g}$ is in the domain of $\tilde{W}_{k',k}$, then the state $|\gamma, h, s'\rangle_{k,g} = \tilde{W}_{k',k}|\gamma, h, s\rangle_{k,g}$ represents the same number in base k' as $|\gamma, h, s\rangle_{k,g}$ does in base k .

This shows that one can proceed in two ways: Arbitrarily choose both $\mathcal{B}_{k,g}$ and $\mathcal{B}_{k',g}$ and define $\tilde{W}_{k',k}$ to be a map from $\mathcal{B}_{k,g}$ to $\mathcal{B}_{k',g}$. Alternatively choose $\mathcal{B}_{k,g}$ and a definition of $\tilde{W}_{k',k}$ and let $\mathcal{B}_{k',g}$ be the range set of $\tilde{W}_{k',k}$.

These methods work only if k and k' have the same prime factors. If this is not the case, one can extend the definition of $\tilde{W}_{k',k}$ by use of definitions to accuracy ℓ , much as was done for the division operator.

There is another quantum theory representation of real and complex numbers that is based on operators instead of sequences of states of q_k strings. To define these operators one replaces the natural number domain of sequences Ψ by states of finite q_k strings that represent natural numbers. In this way the sequences Ψ

¹⁷Recall that each g is a function from $I \times I$ to a basis set for a k dimensional Hilbert space associated with each element of $I \times I$.

¹⁸ $\mathcal{B}_{k,g}$ and $\mathcal{B}_{k',g}$ are each a set of states of all finite tuples of states of finite length quikit strings for bases k and k' .

become quantum operators O where

$$(93) \quad \Psi(n) = O|+, h, n\rangle_{k,g}.$$

Here $|+, h, n\rangle_{k,g}$ denotes a qukit string state $|+, h, s\rangle_{k,g}$ in $\mathcal{B}_{k,g}$ that represents the number n in base k .¹⁹ Note that Eq. 93 holds irrespective of whether Ψ is a $\mathcal{B}_{k,g}$ valued or a more general \mathcal{F}_k valued sequence.

One can use Eq. 93 to replace state sequences by operators. The definition of the Cauchy condition can be changed to apply to these operators by quantifying over the states $|+, h, n\rangle_{k,g}$ as natural number representations and replacing the state $|\gamma_j, h_j, s_j\rangle_{k,g}$ in Eq. 34 by $O|+, h, j\rangle_{k,g}$ and the state $\Psi(j)\rangle$ in Eq. 35 by $O|+, h, j\rangle_{k,g}$. Similar replacements are made for $|\gamma_m, h_m, s_m\rangle_{k,g}$ and $\Psi(m)\rangle$. Operators that satisfy the relevant Cauchy condition are denoted here as Cauchy operators.

The rest of the definition of quantum theory representations of real and complex numbers can be taken over to define representations as equivalence classes of Cauchy operators. In that case there does not seem to be a reason why one could not extend the frame field description to apply to Cauchy operators. An observer in a frame would see real valued physical quantities in an immediate descendant frame as equivalence classes of Cauchy operators.

It is clear that there is much to do, both in understanding the representations of theories in the frame fields and in integrating this work with physics. In any case it is seen that quantum representations of real and complex numbers as equivalence classes of Cauchy sequences of states of qukit strings are different from the usual classical representations. Not only are the quantum equivalence classes larger than the classical ones but the space of representations enjoys two degrees of freedom not present in the space of classical representations. These are the gauge freedom and the iteration stage freedom. The freedom of base choice is present in both quantum and classical representations.

Acknowledgement

This work was supported by the U.S. Department of Energy, Office of Nuclear Physics, under Contract No. DE-AC02-06CH11357.

References

- [1] E. Wigner, *Commun. Pure and Applied Math.* **13** 001 (1960), Reprinted in E. Wigner, *Symmetries and Reflections*, (Indiana Univ. Press, Bloomington IN 1966), pp222-237.
- [2] R. W. Hamming, *Amer. Mathematical Monthly*, **87**, No 2, February, (1980).
- [3] *The Role of Mathematics in Physical Sciences: Interdisciplinary and Philosophical Aspects*, G. Boniolo, P. Budinich, M. Trobok, Eds, Springer Publications, Dordrecht, the Netherlands, 2005.
- [4] P. Benioff, *Found. Phys.* **32**, 989-1029, (2002) [arxiv:quant-ph/0201093].
- [5] P. Benioff, *Found. Phys.* **35**, 1825-1856, (2005) [arxiv:quant-ph/0403209].
- [6] P. Benioff, *Intl Jour. Pure, Applied Math.* **39**, 297-341, (2007), [arxiv:quant-ph/0508219].
- [7] P. Benioff, *Jour. Phys. Conference Series*, **70**, 012003 (2007), [arXiv: quant=ph/0611139]; arXiv: quant-ph/0604135.

¹⁹Here for simplicity, $|+, h, s\rangle_{k,g}$ is assumed to be a state with no leading or trailing 0s. This can easily be relaxed, if desired.

- [8] M. Tegmark, arXiv:0704.0646.
- [9] M. Tegmark, Ann. Phys. (NY) **270**, 1, (1998) [gr-qc/9704009].
- [10] D. Finkelstein, Quantum Relativity. Springer-Verlag, Heidelberg (1996).
- [11] K.-G. Schlesinger, Journal of Mathematical Physics, **40**, 1344-1358 (1999).
- [12] S. Titani and H. Kozawa, Internat. Jour. Theoret. Phys. **42**, 2575-2602, (2003).
- [13] G. Takeuti, *Two Applications of Logic to Mathematics* Kano Memorial Lecture 3, Princeton University Press, New Jersey, 1978; *Quantum set theory*, in: E. G. Beltrametti, B. C. van Fraassen, Eds., *Current issues in quantum logic*, Plenum, pp. 303-322, New York 1981.
- [14] M. Ozawa, J. Symbolic Logic **72**, 625-648, (2007), [arxiv:math.LO/0604.349].
- [15] K. Tokuo, Int. Jour. Theoretical Phys., **43**, 2461-2481, 2004.
- [16] J. V. Corbett and T. Durt, arXiv:quant-ph/0211180 v1 2002.
- [17] M. Davis, Internat. Jour. Theoret. Phys. **16**, 867-874, (1977).
- [18] E. I. Gordon, Soviet Math. Dokl. **18**, 1481-1484 (1977).
- [19] G. L. Litvinov, V. P. Maslov, and G. B. Shpiz, Archives preprint, quant-ph/9904025, v5, 2002.
- [20] A. Doering and C. J. Isham, arXiv:quant-ph/0703060; arXiv:quant-ph/0703062; arXiv:quant-ph/0703064; arXiv:quant-ph/0703066.
- [21] J. Krol, "A Model of Spacetime. The Role of Interpretations in Some Grothendieck Topoi", preprint, (2006).
- [22] S. Lloyd, Phys. Rev. Lett. **88**, 237901, (2002).
- [23] P. C. Davies, arXiv:quant-ph/0703041.
- [24] S. D. H. Hsu, International J. Modern Phys. A **22**, 2895-2907, (2007).
- [25] E. Hewitt and K. Stromberg, *Real and Abstract Analysis* Springer Verlag, Inc. New York, 1965.
- [26] J. C. Burkhill and H. Burkhill, *A second Course in Mathematical Analysis*, Cambridge University Press, Great Britain, 1970.
- [27] Y. Aharonov and T. Kaufherr, Phys. Rev. D **30**, 368-385, (1984).
- [28] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. A **70**, 032307 (2004).
- [29] P. Benioff, arXiv:0704.3574 [quant-ph].
- [30] S. J. van Enk, Phys. Rev. A **71**, 032339 (2005).
- [31] S. J. van Enk, Phys. Rev. A **73** 042306 (2006) [arxiv:quant-ph/0602079].
- [32] D. Poulin and J. Yard, arxiv:quant-ph/0612126.
- [33] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555-609 (2007).
- [34] P. Benioff, Phys. Rev. A **64**, 052310 (2001) [arXiv:quant-ph/0104061v3].
- [35] J. Barwise, "An Introduction to First Order Logic" in Handbook of Mathematical Logic, J. Barwise, Ed. Studies in Logic and the Foundations of Mathematics, Vol. 90. North Holland Publishing Co. New York, 1977, pp 5-46.
- [36] J. F. Randolph, *Basic Real and Abstract Analysis*, Academic Press, New York, 1968.
- [37] J. R. Shoenfield, *Mathematical Logic*, Addison Weseley, Reading, Ma. 1967.
- [38] T. J. Jech, *Lectures in Set theory with Particular Emphasis on the Method of Forcing*, Lecture Notes in Mathematics No. 217 Springer Verlag New York 1971.
- [39] *The Quantum Structure of Space and Time*, Proceedings of the 23rd Solvay Conference, Brussels, Belgium, Dec. 1-3, 2005, D. Gross, M. Henneaux, A. Sevrin, Eds., World Scientific Press, New Jersey.
- [40] A. Ashtekar and J. Lewandowski, Classical and Quantum Gravity, **21**, R53-R152, (2004).
- [41] B. Zweibach, *A First Course in String Theory*, Cambridge Univ. Press, New York, N. Y. 2004.
- [42] G. 't Hooft, Class. Quant. Grav. **13** 1023-1040 (1996) [arXiv:gr-qc/9601014].
- [43] Y. J. Ng and H. van Dam, Int J. Mod. Phys. A **20**, 1328-1335, (2005) [arXiv:gr-qc/0403057]; arXiv:gr-qc/9906003.
- [44] R. Gambini and J. Pullin, arXiv:gr-qc/0505023.
- [45] B. G. Sidharth, arXiv:physics/0402007.
- [46] S. Hossenfelder, arXiv:hep-th/0603032.
- [47] A. Kempf and R. Martin, arXiv:0708.0062.
- [48] M. Maziashvili, arXiv:0708.1472.

- [49] M. S. Byrd, D. Lidar, Lian-Ao Wu, and P. Zanardi, Phys. Rev. A **71**, 052301 (2005).
- [50] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).
- [51] N. Mukunda, G. Marmo, A. Zampini, S. Chaturvedi, and R. Simon, Jour. Math. Phys. **46**, 012106 (2005).
- [52] S. F. Novaes, arXiv:hep-th/0001283;
- [53] A. N. Cottingham and D. A. Greenwood, *An Introduction to the Standard Model of Physics*, Cambridge University Press, Cambridge, UK, 1998.

PHYSICS DIVISION, ARGONNE NATIONAL LABORATORY, ARGONNE, IL 60439, USA

E-mail address: `pbenioff@anl.gov`

This page intentionally left blank

Two paradigms for topological quantum computation

Eric C. Rowell

ABSTRACT. We present two paradigms relating algebraic, topological and quantum computational statistics for the topological model for quantum computation. In particular we suggest correspondences between the computational power of topological quantum computers, computational complexity of link invariants and images of braid group representations. While at least parts of these paradigms are well-known to experts, we provide supporting evidence for them in terms of recent results. We give a fairly comprehensive list of known examples and formulate two conjectures that would further support the paradigms.

1. Introduction

Topological quantum computation (TQC) is expected to be physically realized on quantum systems in *topological phases*. For example, the quasi-particle excitations in fractional quantum hall liquids are conjectured to exhibit the topological behavior necessary to support TQC. A definition of topological phase is found in [3]: “...a system is in a topological phase if its low-energy effective field theory is a topological quantum field theory (TQFT)”. Thus all observable properties of topological phases should be expressible in terms of the structure of the corresponding TQFT. On the other hand, it is known [39] that *modular categories* faithfully encode (3D) TQFTs in algebraic terms. These relationships between modular categories, TQFT, topological phases and topological quantum computers are illustrated in Figure 1. The solid arrows represent well-established or (tautological) one-to-one correspondences, while the dashed arrows represent theoretical expectations.

While the algebraic axioms defining modular categories may seem quite distant from condensed matter physics and quantum computation, certain natural statistics in modular categories appear to correspond to important computational properties in TQC. Most significantly, the images of the braid group representations associated to a modular category are intimately related to the computational power (*universality*) of the corresponding TQC. We illustrate this with two well-known examples:

EXAMPLE 1.1. Consider the (unitary) modular category $\mathcal{C}(\mathfrak{sl}_2, e^{\pi i/5})$ obtained as a subquotient of the representation category of the quantum group $U_q \mathfrak{sl}_2$ with

2000 *Mathematics Subject Classification.* Primary 81P68; Secondary 20F36, 57M25, 68Q17, 57M27.

Key words and phrases. quantum computation, braid group, modular category, link invariant.

©2009 American Mathematical Society

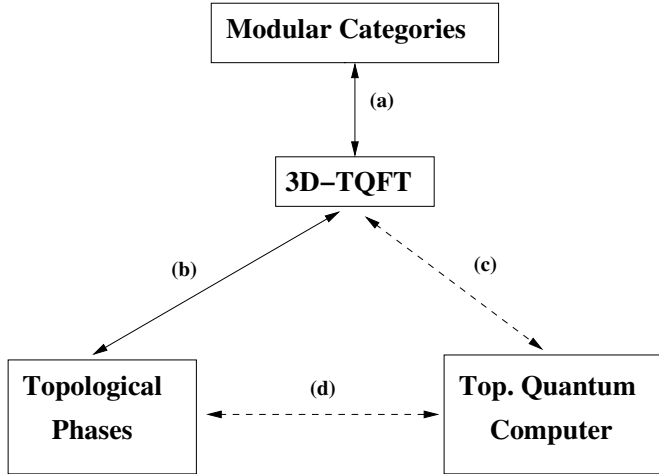


FIGURE 1. (a) equivalent by [39], (b) essentially by definition, see [3], (c) idea originated in [11], (d) first described in [26]

$q = e^{\pi i/5}$ (associated with the $SU(2)$ -Chern-Simons-Witten TQFT at level 3). We note the following:

- (1) The images of the associated braid group representations are as large as possible, i.e. *dense* in the group of special unitaries [13].
- (2) A topological quantum computer realized upon a physical system algebraically modeled by $\mathcal{C}(\mathfrak{sl}_2, e^{\pi i/5})$ is *universal* [13], that is, any unitary matrix can be approximately achieved to a prescribed precision in an efficient way as a product of the matrices representing the braid group generators.
- (3) The associated link invariant is $J_L(e^{2\pi i/5})$ the Jones polynomial evaluated at q^2 , which has computational complexity $\#P$ -hard [19].

Moreover, approximate computation of the Jones polynomial at a 5th root of unity is known to be BQP -complete, so that it is essentially the hardest problem any quantum computer can hope to solve.

EXAMPLE 1.2. Consider the (unitary) modular category $\mathcal{C}(\mathfrak{sl}_2, e^{\pi i/4})$ obtained as a subquotient of the representation category of the quantum group $U_q \mathfrak{sl}_2$ with $q = e^{\pi i/4}$ (associated with the $SU(2)$ -Chern-Simons-Witten TQFT at level 2). We note the following:

- (1) The images of the associated braid group representations factor over finite groups [20].
- (2) A topological quantum computer realized upon a physical system algebraically modeled by $\mathcal{C}(\mathfrak{sl}_2, e^{\pi i/4})$, while highly-entangling (see [9], [25]) is not universal.
- (3) The associated link invariant is (some normalization of) $J_L(i)$ the Jones polynomial evaluated at $q^2 = i$, which can be computed in polynomial time [19].

Two paradigms based upon these examples might then associate density of the braid group image with universal quantum computers and $\#P$ -hard computational

problems, and finite braid group images with non-universal (but potentially entangling) quantum devices and polynomial-time computational problems. Indeed, all evaluations of the Jones, HOMFLYPT and Kauffman link invariants that are polynomial-time computable on a classical computer are associated with “classical” link invariants (see [40, Theorems 6.3.2, 6.3.5 and 6.3.6]), by which we mean link invariants pre-dating quantum topology. Moreover, the corresponding braid group images in these cases have been shown to be finite in essentially all cases (see [14], [16], [29], [28], [20]). However, a deeper examination of further examples reveals that this is not quite correct and a slight refinement is necessary.

In this paper we intend to describe such a refinement of these two paradigms. Our aim is three-fold: to give paradigms that can be of theoretical value to physicists, to describe a few conjectures of mathematical interest, and to present one perspective on the landscape of inter-related fields represented in the topological quantum computation endeavor.

Any attempt to be fully self-contained would require the introduction of many concepts from category theory, low-dimensional topology, complexity theory and condensed matter physics. For brevity’s sake, we will content ourselves with providing the reader with a few references. For an excellent survey of the physical and theoretical set-up for TQCs, see [3]. For the categorical and topological concepts, see [1] and [39]. For complexity theory applied to topological invariants, see [40].

Acknowledgments. The author would like to thank the following people for their generosity in valuable correspondence and conversations: S. Witherspoon, L. Goldberg, Y. Zhang, J. Ospina, S. Stirling, M. Rojas, A. Bulatov, Z. Wang, G. Kuperberg, T. Stanford, and M. Thistlethwaite.

2. Background

We briefly describe some of the important features of modular categories and their relationships with topological phases, link invariants and topological quantum computers.

A unitary modular category (UMC) \mathcal{C} is a semisimple \mathbb{C} -linear rigid ribbon category of finite rank satisfying a certain non-degeneracy condition, such that the morphism spaces are equipped with a positive definite hermitian form compatible with the other structures. The representation category of a finite group is an example of a category that satisfies all but one of the defining axioms of unitary modular tensor categories: namely it fails the *modularity* (non-degeneracy) condition. UMCs are constructed in a diversity of ways from various fields of mathematics.

2.1. Constructions of UMCs. Often very different constructions yield equivalent categories, so we will only list a few well-known explicit constructions.

- (1) **Quantum groups.** To any finite dimensional simple Lie algebra \mathfrak{g} and a root of unity $q = e^{\pi i/\ell}$ one may associate a pre-modular category $\mathcal{C}(\mathfrak{g}, q)$. These are obtained as subquotients of the category of finite dimensional representations of the quantum group $U_q\mathfrak{g}$, see [36] for a survey. Such a category may fail to be modular or unitary (see [35] and [37]), but such circumstances can be avoided by certain restrictions on ℓ . Specifically, define $m = 1$ for Lie types A, D and E , $m = 2$ for Lie types B, C and F_4 and $m = 3$ for Lie type G_2 . Then $\mathcal{C}(\mathfrak{g}, q)$ is a UMC provided $m \mid \ell$ (see [42]).

- (2) **Finite groups.** Fix a finite group G and a 3-cocycle ω . Then the twisted double of G , $D^\omega G$, is a finite dimensional quasi-triangular quasi-Hopf algebra. The representation category $\text{Rep}(D^\omega G)$ is always a UMC, see [1] for details.
- (3) **Doubled spherical categories.** There is a doubling procedure from which one obtains a modular category $\mathcal{Z}(\mathcal{S})$ from a *spherical category* \mathcal{S} (see [2] for the precise definition, and [33] for the double construction). Briefly, a spherical category is a tensor category that is not necessarily braided but for which one has a canonical trace function. Examples are ribbon categories and certain categories obtained from von Neumann algebras (see [18] for a description of the latter). In fact, the representation categories of twisted doubles of finite groups can be obtained as the double of the spherical category $\text{Rep}(\mathbb{C}[G])$ of representations of the group algebra of G . Very few explicit “new” examples of modular categories obtained in this way have been worked out. A few infinite families can be found in [18], and the analysis of two examples are worked out in detail in [17]. If the spherical category \mathcal{S} is unitary the double $\mathcal{Z}(\mathcal{S})$ will be a UMC.

2.2. Braid Group Representations. The axioms of a UMC imply that for any object X in a UMC \mathcal{C} one obtains a (highly non-degenerate) unitary representation $\phi_X^n : \mathcal{B}_n \rightarrow \text{U}(\text{End}(X^{\otimes n}))$. Recall that \mathcal{B}_n , the braid group on n -strands, is the group with $n - 1$ generators $\sigma_1, \dots, \sigma_{n-1}$ satisfying:

$$(B1) \quad \sigma_i \sigma_j = \sigma_j \sigma_i \text{ if } |i - j| \geq 2$$

$$(B2) \quad \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \text{ for } 1 \leq i \leq n - 2.$$

The braiding on \mathcal{C} requires that there are natural braiding isomorphisms $C_{X,Y} : X \otimes Y \cong Y \otimes X$. In particular one obtains natural isomorphisms

$$R_X^i := Id_X^{\otimes(i-1)} \otimes C_{X,X} \otimes Id_X^{\otimes(n-i-1)} \in \text{End}(X^{\otimes n})$$

so that the left action of $\text{End}(X^{\otimes n})$ on itself induces the representation ϕ_X^n by

$$\phi_X^n(\sigma_i) f = R_X^i \circ f.$$

The unitarity of ϕ_X^n is due to the fact that $\text{End}(X^{\otimes n})$ is a Hilbert space, the naturality of the braiding isomorphisms and the compatibility of the hermitian form with the other structures.

Given such a representation it is natural to ask

QUESTION 2.1. What is the closure of $\phi_X^n(\mathcal{B}_n)$ in $\text{U}(\text{End}(X^{\otimes n}))$?

Indeed, this question was asked by Jones in [20] long before its relevance to quantum computing was realized.

Let us suppose that we have a decomposition $\text{End}(X^{\otimes n}) = \bigoplus_k V_k$ into irreducible \mathcal{B}_n -representations, and fix one irreducible subrepresentation V_k . Denote by Γ_k the closure of the image of \mathcal{B}_n in $\text{U}(V)$. Then Γ_k modulo its center is exactly one of the following:

- (1) A finite abelian group
- (2) A finite non-abelian group
- (3) An infinite compact group containing $\text{SU}(V)$
- (4) An infinite compact group not containing $\text{SU}(V)$

These motivate the following:

- DEFINITION 2.2. (1) If $\Gamma_k/Z(\Gamma_k)$ is always a finite group for all objects X in \mathcal{C} , all $n \in \mathbb{N}$, and all irreducible subrepresentations $V_k \subset \text{End}(X^{\otimes n})$ then we say \mathcal{C} has **property F**.
- (2) If there exists an object X in \mathcal{C} and $N \in \mathbb{N}$ such that for all $n \geq N$ and for each irreducible subrepresentation $V_k \subset \text{End}(X^{\otimes n})$ the group $\Gamma_k/Z(\Gamma_k)$ contains $\text{SU}(V_k)$ we say \mathcal{C} has the **density property**.

In nearly all cases one encounters in the literature, \mathcal{C} has either property **F** or the density property (see e.g. [20], [14], [29], [7] and [28]).

REMARK 2.3. One may generalize the construction above in the following way. The *pure braid group* \mathcal{P}_n is the (normal) subgroup of \mathcal{B}_n generated by the conjugacy class of σ_1^2 , or equivalently, the kernel of the obvious homomorphism $\mathcal{B}_n \rightarrow S_n$ that sends σ_i to the transposition $(i, i+1)$. So geometrically \mathcal{P}_n consists of the braids whose strands begin and end at the same position. Now fix any set of n objects $X_{i(1)}, \dots, X_{i(n)}$. Then \mathcal{P}_n acts on $\text{End}(\bigotimes_j X_{i(j)})$ in the obvious way using the braiding operators of the form $C_{Y,X}C_{X,Y}$ and their conjugates. One might ask if the image of \mathcal{P}_n is finite or infinite for all n and all choices of $X_{i(j)}$. But this is not a more general question: If we define $X = \bigoplus_j X_{i(j)}$ then if \mathcal{C} has property **F**, \mathcal{B}_n has finite image on $\text{End}(X^{\otimes n})$, so that by restricting to \mathcal{P}_n and to the subspace $\text{End}(\bigotimes_j X_{i(j)}) \subset \text{End}(X^{\otimes n})$, one sees that the \mathcal{P}_n image is finite as well. Obviously the converse is true as well: since \mathcal{P}_n has finite index, we may take $X_{i(j)} = Y$ for all j and so finiteness of the \mathcal{P}_n image implies finiteness of the \mathcal{B}_n image. Similar statements can be made if we replace \mathcal{P}_n by any finite index subgroup of \mathcal{B}_n obtained as a pull-back of a subgroup of S_n via the homomorphism above. For example, the subgroup of \mathcal{B}_n generated by those elements with the first strand beginning and ending at the same vertical position is the pull-back of the subgroup of S_n that fixes 1.

2.3. Link Invariants. Associated to any modular category \mathcal{C} is a 3D-TQFT, which gives rise to 3-manifold and link invariants. In essence the link invariants are obtained by representing a link L as the closure of a braid $\beta \in \mathcal{B}_n$, and then taking the trace of the image of β in one of the representations ϕ_X^n of \mathcal{B}_n described above. More generally, one colors each component of L with objects $X_{i(j)}$ of \mathcal{C} and represents the colored link as the closure of a braid γ where the strands of γ must respect the given coloring. Then one takes the trace of the image of γ in the appropriate endomorphism space. See [39, Chapter II] for full details. There are two standard choices that will appear below. We consider the invariants corresponding to coloring all components with either a fixed simple object X_i or the sum of all simple objects. One caveat for what follows: the link invariants we discuss can be derived in a number of different ways, each of which has a preferred normalization. These normalizations do not affect the computational complexity class of the invariants, so we do not concern ourselves with being to precise in this regard. The same warning applies to Table 3.3.5.

The link invariants associated to the modular categories mentioned above are as follows, where $q = e^{\pi i/\ell}$:

- (1) The link invariant associated to $\mathcal{C}(\mathfrak{sl}_2, q)$ where we color each component with the object analogous to the irreducible 2-dimensional representation of \mathfrak{sl}_2 is the Jones polynomial $J_L(q^2)$.

- (2) More generally, the link invariant associated to $\mathcal{C}(\mathfrak{sl}_n, q)$ is a one-variable specialization of the (reparameterized) HOMFLYPT polynomial $P'_L(q, n)$. As above, the invariant P'_L corresponds to coloring each strand with the object analogous to the n -dimensional representation of \mathfrak{sl}_n . In the setting of Hecke algebras, this corresponds to the n -row quotient.
- (3) Consider the category $\mathcal{C}(\mathfrak{g}, q)$ where \mathfrak{g} is of Lie type B, C or D , and in the first two cases ℓ is even, and let X be the object analogous to the vector representation of \mathfrak{g} . Then the invariant associated to X is a specialization of the (Dubrovnik version) of the Kauffman polynomial $F_L(q^k, q)$, where k depends on the rank of \mathfrak{g} .
- (4) Link invariants associated with $\mathcal{C}(\mathfrak{g}, q)$ for \mathfrak{g} of other Lie types have not been extensively studied, nor have invariants associated with objects other than those analogous to the vector representation. There are two exceptions. Explicit skein relations have been worked out by G. Kuperberg for Lie type G_2 . Also, the invariant associated with the object analogous to the fundamental spin representation of \mathfrak{so}_p in $\mathcal{C}(\mathfrak{so}_p, q)$ with $\ell = 2p$, p an odd prime is known to be related to the homology modulo p of the double cyclic cover M_L of S^3 branched over the given link L (see [4] and [16]).
- (5) The link invariants associated to the modular categories $\text{Rep}(D^\omega G)$ with $\omega = 0$ are described in [10]. Specifically, if we color each component of L with the sum of the simple objects (or with DG itself), one gets (a normalization of) the classical link invariant

$$H_L(G) = |\text{Hom}(\pi_1(S^3 \setminus L), G)|.$$

That is, for a fixed link L it counts the homomorphisms from the fundamental group of the link-complement to the finite group G .

- (6) the TQFTs associated with doubled spherical categories are usually called Turaev-Viro(-Ocneanu) TQFTs. The associated link invariants are not well-studied, although some attention has been paid to two of these “exotic” examples, see [17].

Later the computational complexity of evaluating these link invariants will be discussed. Two important complexity classes are FP and $\#P$. The class of functions that are computable in polynomial time in the length of the input are of complexity FP , which is most closely associated with decision problems of complexity P . The class of counting functions of complexity $\#P$ are related to decision problems of complexity NP , where instead of asking if there exists a “yes” answer one counts the number of “yes” answers. For example, deciding if a given Boolean expression E has an assignment of truth values that satisfy E is NP -complete, while counting the number of such assignments is $\#P$ -complete.

3. The Paradigms

The two paradigms are shown in Figures 2 and 3 respectively. Each has three boxes representing braid group images, complexity of link invariants, and utility in quantum computation. Our limited expertise in physics led us to exclude any corresponding speculations from the paradigm, however, see Remark 3.3 below.

3.1. Dense Image Paradigm. In Figure 2, “Braid group image dense” represents those unitary modular categories which have the density property.

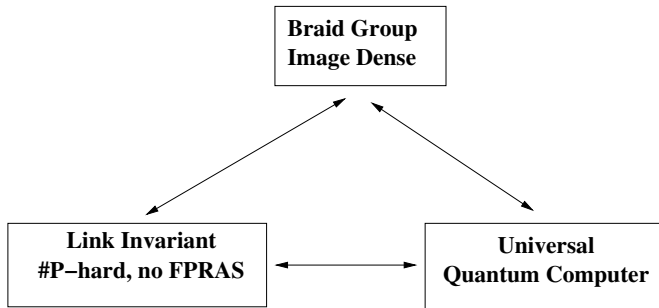


FIGURE 2. Dense Image Paradigm

The “Link invariant” box requires some explanation. We say computation of the link invariants are $\#P$ -hard because in each known case the exact computation of the invariant can be reduced to a counting problem. For example, an evaluation of the Jones polynomial of a link L at a root of unity q^2 is an integer linear combination of the Galois conjugates of q , so that computing each coefficient may be regarded as a counting problem. That such an evaluation is *hard* means that if we could find an efficient algorithm for such a problem, we could (in principle) adapt our algorithm to efficiently solve any $\#P$ problem. However, comparing the quantum computation of a link invariant to classical exact computation is at some level unrealistic for at least two reasons: 1) quantum computation is probabilistic, while classical computation is deterministic and 2) most quantum computations will involve approximate application of some quantum gate (unitary operator), so that the output will be an approximate evaluation as well. A more relevant question to ask is: does a link invariant f have a *fully polynomial randomized approximation scheme* (FPRAS)? That is, does there exist an algorithm whose input is a link L with braid index at most n and an error threshold $\varepsilon > 0$, whose output is a number Y so that

$$Pr\left(\frac{1}{1+\varepsilon} \leq \frac{Y}{f(L)} \leq 1+\varepsilon\right) > 3/4$$

that runs in polynomial time in n and $1/\varepsilon$? Of course by running such an algorithm multiple times, one may improve the certainty that the approximation of $f(L)$ is correct within an ε factor of $f(L)$. The associated decision problem complexity class is RP (*randomized polynomial time*). It is widely believed that $RP \neq NP$, and the non-existence of an *FPRAS* for a given problem is usually proved under this assumption.

Finally, by “Universal Quantum Computer” we mean that the set of matrices representing the braid group generators form a universal gate set, see [13] for a more explicit description.

3.2. Finite Image Paradigm. Most of the relationships in the Finite Image paradigm (Figure 3) can be understood from the remarks on the Dense Image paradigm above. Notice that we have excluded the finite abelian braid group images from the description. This is because the cases where the images of the braid group are finite abelian are mathematically trivial, corresponding to *abelian anyons*. Firstly, the link invariant will essentially count components or at best

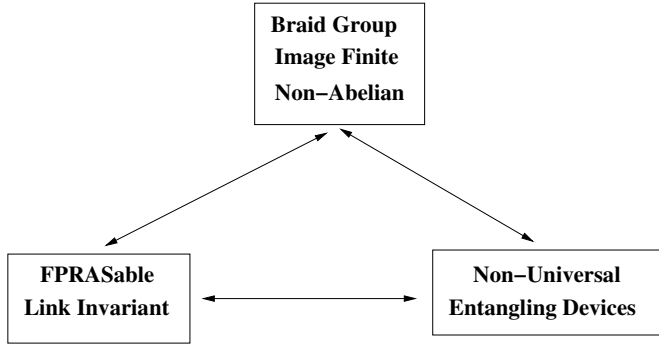


FIGURE 3. Finite Image Paradigm

linking numbers, which can be done classically in polynomial time. Secondly, the representations of the braid group in these cases are all 1-dimensional. Because of this, there is no ground state degeneracy and hence any device based upon such systems would not even be capable of efficiently storing information, i.e. they would be non-entangling. It is interesting to note that, to date, the only topological phases that have been convincingly shown to exist are abelian anyons (see [3]).

Non-universal quantum devices that can at least produce entangled qubits could potentially be used to store quantum information and even be useful in quantum error correction (see e.g. [43]). A well-known example is the Bell basis change matrix which is related to the Jones polynomial at $t = i$.

3.3. Evidence. Analyses of the braid group images and the computational complexity of the link invariant evaluations associated to many of the modular categories described above have been carried out. We discuss each in turn, recording the precise evidence for the two paradigms in Table 3.3.5 where speculations are in bold type. For notational convenience, set $q = e^{\pi i/\ell}$, and denote by c the number of components of a link L . Let d_k be the dimension of the homology space modulo k of the double cyclic cover of S^3 branched over L . $K(L)$ is a classical invariant that only depends on the linking matrix of L .

3.3.1. Jones polynomial. For $\mathcal{C}(\mathfrak{sl}_2, q)$ with $q = e^{\pi i/\ell}$, $3 \leq \ell$ and X_1 the object corresponding to the fundamental 2-dimensional representation of \mathfrak{sl}_2 the algebra $\text{End}(X_1^{\otimes n})$ is isomorphic to the Temperley-Lieb algebra $TL_n(q^2)$. Jones determined precisely when the braid group images are finite in [20], and in all other cases it is shown in [14, Theorem 0.1] that the braid group images are dense. The (exact) computational complexity of the corresponding link invariant the Jones polynomial $J_L(q^2)$ was worked out in [19], where it is shown that, except for $\ell \in \{1, 2, 3, 4, 6\}$ the complexity class is $\#P$ -hard. This was accomplished by using a result of Thistlethwaite that evaluating the Jones polynomial at $t = q^2$ for L an alternating link is essentially equivalent to computing the Tutte polynomial of an associated plane graph $G(L)$ at $(-t, -1/t)$, which is shown to be $\#P$ -hard except at the special points described above. The Jones polynomial at these special points degenerates to a “classical” link-invariant that is computable in polynomial time. We conjecture the following:

CONJECTURE 3.1. There is no FPRAS for evaluating $J_L(q^2)$ except at the special points described above, provided $RP \neq NP$.

This conjecture is partially motivated by the belief that quantum computers are strictly more powerful than classical computers. If this conjecture were false, there would be an *FPRAS* for a *BQP*-complete problem. A second, less philosophical, piece of evidence is found in [15], where it is shown that, away from the positive quadrant in the rational xy -plane and a few exceptional curves, no *FPRAS* exists for evaluating the Tutte polynomial at (x, y) . This result does not apply to complex pairs (x, y) and so does not give any information for the Jones polynomial at roots of unity, but is nonetheless compelling evidence for our conjecture.

3.3.2. HOMFLYPT polynomial. Generalizations of the results above to the categories $\mathcal{C}(\mathfrak{sl}_n, q)$ with $q = e^{\pi i/\ell}$ and the corresponding specializations of the HOMFLYPT polynomial are found in [40] (due to Vertigan), [14], and [16]. The role of the Temperley-Lieb algebra is taken by specializations of the two-parameter Hecke-algebra (see [21]), and the results are of the same format with one exception: for $n \geq 3$ one may have infinite braid group images that are not dense, see [14, Theorem 4.1]. See also [34] for a related invariant obtained by summing over all colorings, for which it is shown that one essentially obtains $\pm \sqrt{H_L(G)}$ (see below), with G abelian.

Since the Jones polynomial can be obtained as a specialization of the HOMFLYPT polynomial, FPRASability of the HOMFLYPT polynomial would imply the same for the Jones polynomial.

3.3.3. Kauffman polynomial. The computational complexity of evaluating the Kauffman polynomial has been worked out by Vertigan, see [40]. The relevant modular categories are obtained from the categories of the form $\mathcal{C}(\mathfrak{g}, q)$ with $\mathfrak{g} \in \{\mathfrak{so}_N, \mathfrak{sp}_{2N}\}$. In these cases the algebras $\text{End}(X^{\otimes n})$ are related to specializations of the form $r = q^k$ of *BMW*-algebras $C_n(r, q)$ (see [41, Prop. 2.1]), where as usual X is the quantum analogue of the vector representation. The braid group images are worked out in all non-trivial cases except $r = \pm i$ in [22], [29], [28] and [8]. In general the images are either finite or dense, although exceptions are found in [28], and are expected for $r = \pm i$.

Again, as the Jones polynomial can be obtained as a specialization of the Kauffman polynomial, FPRASability of the Kauffman polynomial would imply the same for the Jones polynomial.

3.3.4. $\mathbf{d_n} = \dim \mathbf{H_1(M_L, \mathbb{Z}_n)}$. The categories $\mathcal{C}(\mathfrak{so}_{2n+1}, e^{\pi i/\ell})$ with $\ell = 2(2n + 1)$ may be regarded as the extension of the series of modular categories whose first two terms are $\mathcal{C}(\mathfrak{sl}_2, e^{\pi i/6})$ and $\mathcal{C}(\mathfrak{sp}_4, e^{\pi i/10})$. At least for $2n + 1 = p \geq 7$ prime, the corresponding link invariants are $\pm(\sqrt{p})^{d_p}$ where $d_p = \dim H_1(M_L, \mathbb{Z}_p)$ with M_L the double cyclic cover of S^3 branched over L , see [16] and [4]. Polynomial algorithms exist for computing the dimension of these homology spaces, and the braid group images are shown to be finite (symplectic) groups in [16]. It seems reasonable that this should hold for arbitrary $2n + 1$ as well.

3.3.5. $\mathbf{H_L(G) = |\text{Hom}(\pi_1(\mathbf{S^3} \setminus \mathbf{L}), \mathbf{G})|}$. While the fact that the invariant corresponding to the modular category $\text{Rep}(DG)$ for G a finite group is the classical invariant $H_L(G)$ has been known for some time, the computational complexity has not been studied to our knowledge. Moreover, the fact that $\text{Rep}(DG)$ has property F was shown only recently [7].

Recent results suggest the following:

CONJECTURE 3.2. Let G be a finite group and L a link.

- (a) There exists an *FPRAS* for computing $H_L(G)$ for any group G .
- (b) Suppose G is solvable. Then there is a polynomial algorithm for exact computation of $H_L(G)$.

We support this conjecture with the following list of facts:

- (1) Clearly if G is an abelian group and L has k components, then $H_L(G) = |\text{Hom}(H_1(S^3 \setminus L), G)| = |\text{Hom}(\mathbb{Z}^k, G)| = |G|^k$.
- (2) It is shown in [6] that if G is nilpotent and L is a knot then $H_L(G) = |G|$ is constant. So at least for knots, $H_L(G)$ is polynomial time computable for G nilpotent.
- (3) In [32] an algorithm for computing the number of homomorphisms from a given finitely presented group Γ to a finite solvable group is given. It is not clear if this algorithm finishes in polynomial time (in, say, the number of generators of Γ), but it certainly supports the case for (b). Moreover, in preliminary computations (worked out with S. Witherspoon) for G a generalized dihedral group we found that the corresponding braid group representation is equivalent to a finite field evaluation of the Burau representation. This is significant, as the Burau representation supports the Alexander polynomial, which is known to be polynomial-time computable.
- (4) Even in the non-solvable case, an algorithm exists: $\pi_1(S^3 \setminus L)$ has presentation $\langle x_1, \dots, x_n : R_1, \dots, R_m \rangle$ with n and m are bounded by $N + M$ where N is the number of strands in some projection of L and M is the number of crossings. One checks all $|G|^n$ n -tuples against the m relations to find homomorphisms. One could improve this algorithm slightly by applying automorphisms of G , but the algorithm would still be exponential in n . Perhaps a randomization of this algorithm where one samples a moderately-sized subset of the n -tuples of elements of G and then approximates $H_L(G)$ by proportion would provide an *FPRAS*. Whether this could be done efficiently and accurately would require some analysis. We should mention that it is widely believed that an *FPRAS* exists for computing $H_L(G)$ ([27]).

REMARK 3.3. (1) We speculate that an appropriate physical aspect of the paradigm would be as follows: When the braid group image is dense, then it is unlikely that there is an efficient way to approximately simulate the corresponding physical system. Our expertise in the subject is not sufficient to say anything authoritative, but it seems reasonable that an efficient approximate simulation of the physical system could be used to construct an *FPRAS* for the link invariant. When the braid group image is finite, we might expect that efficient numerical methods (such as quantum Monte Carlo) exist for (approximately) simulating the corresponding quantum mechanical systems (see e.g. [23]).

(2) There is a related conjecture characterizing UMCs with property F by the categorical dimensions of their simple objects. This is beyond our current scope, but details will appear in [38].

UMC	Restrictions	Invariant	Complexity	\mathcal{B}_n Image
$\mathcal{C}(\mathfrak{sl}_2, q)$	$5 \leq \ell \neq 6$	$V_L(q^2)$	#P-hard no FPRAS?	dense
$\mathcal{C}(\mathfrak{sl}_n, q)$, $3 \leq n$	$n + 2 \leq \ell$, $\ell \neq 6$	$P'_L(q, n)$	#P-hard no FPRAS?	infinite not dense
$\mathcal{C}(\mathfrak{so}_{2n+1}, q)$, $2 \leq n$	ℓ even, $2n + 2 \leq \ell$, $\ell \neq 4n$	$F_L(q^{2n}, q)$	#P-hard no FPRAS?	dense
$\mathcal{C}(\mathfrak{sp}_{2n}, q)$, $2 \leq n$	ℓ even, $2n + 6 \leq \ell$, $\ell \neq 4n + 2$	$F_L(q^{-2n-1}, q)$	#P-hard no FPRAS?	dense
$\mathcal{C}(\mathfrak{so}_{2n}, q)$, $3 \leq n$	$2n + 2 \leq \ell$, $\ell \neq 4n - 2$	$F_L(q^{2n-1}, q)$	#P-hard no FPRAS?	dense
$\mathcal{C}(\mathfrak{so}_4, q)$	$7 \leq \ell$	$(-1)^{c-1}[V_L(-q^{-2})]^2$	#P-hard no FPRAS?	infinite not dense
$\mathcal{C}(\mathfrak{sl}_2, q)$	$\ell = 3$	$(-1)^{c-1}$	FP	finite abelian
$\mathcal{C}(\mathfrak{sl}_2, q)$	$\ell = 4$	$(-\sqrt{2})^{c-1}(-1)^{\text{Arf}(L)}$ or 0	FP	finite
$\mathcal{C}(\mathfrak{sl}_n, q)$	$\ell = 6$	$\pm(i)^{c-1}(i\sqrt{3})^{d_3}$	FP	finite
$\mathcal{C}(\mathfrak{sp}_4, q)$	$\ell = 10$	$\pm(\sqrt{5})^{d_5}$	FP	finite
$\mathcal{C}(\mathfrak{sl}_n, q)$	$\ell = n + 1$	$e^{\pi i K(L)/n}$	FP	finite abelian
$\mathcal{C}(\mathfrak{so}_p, q)$, $3 \leq p$ prime	X spin rep., $\ell = 2p$	$\pm(\sqrt{p})^{d_p}$	FP	finite
$\text{Rep}(DG)$	G finite	$H_L(G)$	FPRAS?	finite

TABLE 1

References

- [1] B. Bakalov; A. Kirillov, Jr., *Lectures on Tensor Categories and Modular Functors*, University Lecture Series, vol. **21**, Amer. Math. Soc., 2001.
- [2] J. W. Barrett; B. W. Westbury, Spherical categories. *Adv. Math.* **143** (1999), no. 2, 357–375.
- [3] S. Das Sarma; M. Freedman; C. Nayak; S. H. Simon,; A. Stern, Non-Abelian Anyons and Topological Quantum Computation. arXiv:0707.1889.
- [4] J. de Boer; J. Goeree, Markov traces and II_1 factors in conformal field theory. *Comm. Math. Phys.* **139** (1991), no. 2, 267–304.
- [5] R. Dijkgraaf; E. Witten, Topological gauge theories and group cohomology. *Comm. Math. Phys.* **129** (1990), no. 2, 393–429.

- [6] M. Eisermann, The number of knot group representations is not a Vassiliev invariant. *Proc. Amer. Math. Soc.* **128** (2000), no. 5, 1555–1561.
- [7] P. Etingof; E. C. Rowell; S. J. Witherspoon, Braid group representations from quantum doubles of finite groups. *Pacific J. Math.* **234**, no. 1 (2008), 33–41.
- [8] J. Franko, Braid group representations via the Yang Baxter Equation, Ph.D. thesis, Indiana University, 2007.
- [9] J. Franko; E. C. Rowell; Z. Wang, Extraspecial 2-groups and images of braid group representations, *J. Knot Theory Ramifications* **15** (2006) no. 4, 1–15.
- [10] D. Freed; F. Quinn, Chern-Simons theory with finite gauge group. *Comm. Math. Phys.* **156** (1993), no. 3, 435–472.
- [11] Freedman, Michael H. P/NP, and the quantum field computer. *Proc. Natl. Acad. Sci. USA* **95** (1998), no. 1, 98–101 (electronic).
- [12] M. Freedman; A. Kitaev; M. Larsen; Z. Wang, Topological quantum computation. *Bull. Amer. Math. Soc. (N.S.)* **40** (2003), no. 1, 31–38.
- [13] M. Freedman, M. Larsen and Z. Wang, A modular functor which is universal for quantum computation. *Comm. Math. Phys.* **227** (2002), no. 3, 605–622.
- [14] M. H. Freedman; M. J. Larsen; and Z. Wang, The two-eigenvalue problem and density of Jones representation of braid groups. *Comm. Math. Phys.* **228** (2002), 177–199, arXiv: math.GT/0103200.
- [15] L. A. Goldberg; M. Jerrum, Inapproximability of the Tutte polynomial, in *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, 459–468, ACM, New York 2007.
- [16] D. M. Goldschmidt; V. F. R. Jones, Metaplectic link invariants. *Geom. Dedicata* **31** (1989), no. 2, 165–191.
- [17] S.-M. Hong; E. C. Rowell; Z. Wang, On exotic modular tensor categories, to appear in *Commun. Contemp. Math.* arXiv: 0710.5761.
- [18] M. Izumi, The structure of sectors associated with Longo-Rehren inclusions. II. Examples. *Rev. Math. Phys.* **13** (2001), no. 5, 603–674.
- [19] F. Jaeger; D. L. Vertigan; D. J. A. Welsh, On the computational complexity of the Jones and Tutte polynomials. *Math. Proc. Cambridge Philos. Soc.* **108** (1990), no. 1, 35–53.
- [20] V. F. R. Jones, Braid groups, Hecke algebras and type II_1 factors, *Geometric methods in operator algebras (Kyoto, 1983)*, 242–273, Pitman Res. Notes Math. Ser., 123, Longman Sci. Tech., Harlow, 1986.
- [21] V. F. R. Jones, Hecke algebra representations of braid groups and link polynomials. *Ann. of Math. (2)* **126** (1987), no. 2, 335–388.
- [22] V. F. R. Jones, On a certain value of the Kauffman polynomial. *Comm. Math. Phys.* **125** (1989), no. 3, 459–467.
- [23] J. Jordan; R. Orus; G. Vidal; F. Verstraete; J. I. Cirac, Classical simulation of infinite-size quantum lattice systems in two spatial dimensions. arXiv: cond-mat/0703788.
- [24] L. Kauffman, An invariant of regular isotopy. *Trans. Amer. Math. Soc.* **318** (1990), no. 2, 417–471.
- [25] L. Kauffman; S. Lomonaco Jr., Braiding operators are universal quantum gates. *New J. Phys.* **6** (2004), 134.1–134.40 (electronic).
- [26] A. Kitaev, Fault-tolerant quantum computation by anyons. *Ann. Physics* **303** (2003), no. 1, 2–30.
- [27] G. Kuperberg, private communication.
- [28] M. J. Larsen; E. C. Rowell, An algebra-level version of a link-polynomial identity of Lickorish, to appear in *Math. Proc. Cambridge Philos. Soc.*
- [29] M. J. Larsen; E. C. Rowell; Z. Wang, The N -eigenvalue problem and two applications. *Int. Math. Res. Not.* **2005** (2005), no. 64, 3987–4018.
- [30] W. B. R. Lickorish, Some link-polynomial relations. *Math. Proc. Cambridge Philos. Soc.* **105** (1989), no. 1, 103–107.
- [31] S. Lloyd, Quantum computation with abelian anyons. *Quantum Inf. Process.* **1** (2002), no. 1–2, 13–18.
- [32] D. Matei; A. I. Suciu, Counting homomorphisms onto finite solvable groups. *J. Algebra* **286** (2005), no. 1, 161–186.
- [33] M. Müger, *From subfactor to categories and topology, II* J. Pure Appl. Algebra **180** (2003), no. 1–2, 159–219.

- [34] H. Murakami; T. Ohtsuki; M. Okada, Invariants of three-manifolds derived from linking matrices of framed links. *Osaka J. Math.* **29** (1992), no. 3, 545–572.
- [35] E. C. Rowell, On a family of non-unitarizable ribbon categories, *Math Z.* **250** no. 4 (2005) 745–774.
- [36] E. C. Rowell, From quantum groups to unitary modular tensor categories, in *Contemp. Math.* **413** (2006), 215–230.
- [37] E. C. Rowell, Unitarizability of premodular categories, *J. Pure Appl. Algebra*, **212** (2008), no. 8 1878–1887.
- [38] E. C. Rowell, *A finiteness property for braided tensor categories* in preparation.
- [39] V. Turaev, Quantum Invariants of Knots and 3-Manifolds, De Gruyter Studies in Mathematics, Walter de Gruyter 1994.
- [40] D. Welsh, *Complexity: Knots, Colourings and Counting*, LMS Lecture Notes Series 186, Cambridge University Press, Cambridge, 1993.
- [41] H. Wenzl, Tensor categories and braid representations, in *Quantum groups and Lie theory (Durham, 1999)*, 216–234, London Math. Soc. Lecture Note Ser., 290, Cambridge Univ. Press, Cambridge, 2001.
- [42] H. Wenzl, C^* tensor categories from quantum groups. *J. Amer. Math. Soc.* **11** (1998), no. 2, 261–282.
- [43] Y. Zhang; E. C. Rowell; Y.-S. Wu; Z. Wang; M.-L. Ge, From extraspecial two-groups to GHZ states. arXiv:0706.1761.

DEPARTMENT OF MATHEMATICS, TEXAS A& M UNIVERSITY COLLEGE STATION, TX 77845
E-mail address: rowell@math.tamu.edu

This page intentionally left blank

Contraction of Matchgate Tensor Networks on Non-planar Graphs

Sergey Bravyi

ABSTRACT. A tensor network is a product of tensors associated with vertices of some graph G such that every edge of G represents a summation (contraction) over a matching pair of indexes. It was shown recently by Valiant, Cai, and Choudhary that tensor networks can be efficiently contracted on planar graphs if components of every tensor obey a system of quadratic equations known as matchgate identities. Such tensors are referred to as *matchgate tensors*. The present paper provides an alternative approach to contraction of matchgate tensor networks that easily extends to non-planar graphs. Specifically, it is shown that a matchgate tensor network on a graph G of genus g with n vertices can be contracted in time $T = \text{poly}(n) + O(m^3) 2^{2g}$ where m is the minimum number of edges one has to remove from G in order to make it planar. Our approach makes use of anticommuting (Grassmann) variables and Gaussian integrals.

1. Introduction and summary of results

Contraction of tensor networks is a computational problem having a variety of applications ranging from simulation of classical and quantum spin systems [1, 2, 3, 4, 5] to computing capacity of data storage devices [6]. Given the tremendous amount of applications it is important to identify special classes of tensor networks that can be contracted efficiently. For example, Markov and Shi found a linear time algorithm for contraction of tensor networks on trees and graphs with a bounded treewidth [1]. An important class of graphs that do not fall into this category are planar graphs. Although contraction of an arbitrary tensor network on a planar graph is a hard problem, it has been known for a long time that the generating function of perfect matchings known as the *matching sum* can be computed efficiently on planar graphs for arbitrary (complex) weights using the Fisher-Kasteleyn-Temperley (FKT) method, see [7, 8, 9]. It is based on the observation that the matching sum can be related to Pfaffian of a weighted adjacency matrix (known as the Tutte matrix). The FKT method also yields an efficient algorithm for computing the partition function of spin models reducible to the matching sum, most notably, the Ising model on a planar graph [10]. Recently the FKT method has been generalized to the matching sum of non-planar graphs with a bounded genus [11, 12, 13].

2000 *Mathematics Subject Classification.* Primary 11Y16; Secondary 47N55 15A75.

Key words and phrases. matchgate, tensor networks, non-planar graphs.

Computing the matching sum can be regarded as a special case of a tensor network contraction. It is therefore desirable to characterize precisely the class of tensor networks that can be contracted efficiently using the FKT method. This problem has been solved by Valiant [14, 15] and in the subsequent works by Cai and Choudhary [16, 17, 18]. Unfortunately, it turned out that the matching sum of planar graphs essentially provides the most general tensor network in this class, see [16, 18]. Following [16] we shall call such networks *matchgate tensor networks*, or simply *matchgate networks*. A surprising discovery made in [17] is that matchgate tensors can be characterized by a simple system of quadratic equations known as *matchgate identities* which does not make references to any graph theoretical concepts. Specifically, given a tensor T of rank n with complex-valued components $T(x) = T_{x_1, x_2, \dots, x_n}$ labeled by n -bit strings $x \in \{0, 1\}^n$ one calls T a *matchgate tensor*, or simply a *matchgate*, if for all $x, y \in \{0, 1\}^n$

$$(1) \quad \sum_{a: x_a \neq y_a} T(x \oplus e^a) T(y \oplus e^a) (-1)^{x_1 + \dots + x_{a-1} + y_1 + \dots + y_{a-1}} = 0.$$

Here e^a denotes a string in which the a -th bit is 1 and all other bits are 0. The symbol \oplus stands for a bit-wise XOR of binary strings. For example, a simple algebra shows that a tensor of rank $n = 1, 2, 3$ is a matchgate iff it is either even or odd¹. Furthermore, an even tensor of rank 4 is a matchgate iff

$$(2) \quad -T(0000)T(1111) + T(1100)T(0011) - T(1010)T(0101) + T(1001)T(0110) = 0.$$

A matchgate network is a tensor network in which every tensor is a matchgate.

The purpose of the present paper is two-fold. Firstly, we develop a formalism that allows one to perform *partial contractions* of matchgate networks, for example, contraction of a single edge combining its endpoints into a single vertex. More generally, the formalism allows one to contract any connected planar subgraph G of the network into a single vertex $u(G)$ by "integrating out" all internal edges of G . The number of parameters describing the contracted tensor assigned to $u(G)$ is independent of the size of G . It depends only on the number of "external" edges connecting G to the rest of the network. This is the main distinction of our formalism compared to the original matchgate formalism of Valiant [14]. The ability to implement partial contractions may be useful for designing efficient parallel contraction algorithms. More importantly, we show that it yields a faster contraction algorithm for matchgate networks on non-planar graphs.

Our formalism makes use of anticommuting (Grassmann) variables such that a tensor of rank n is represented by a generating function of n Grassmann variables. A matchgate tensor is shown to have a Gaussian generating function that depends on $O(n^2)$ parameters. The matchgate identities Eq. (1) can be described by a first-order differential equation making manifest their underlying symmetry. Contraction of tensors is equivalent to convolution of their generating functions. Contraction of matchgate tensors can be performed efficiently using the standard Gaussian integration technique. We use the formalism to prove that a tensor satisfies matchgate identities if and only if it can be represented by the matching sum on some planar graph. It reproduces the result obtained earlier by Cai and Choudhary [17, 18]. Our approach also reveals that the notion of a matchgate tensor is

¹A tensor T is called even (odd) if $T(x) = 0$ for all strings x with odd (even) Hamming weight.

equivalent to the one of a Gaussian operator introduced in [19] in the context of quantum computation.

Secondly, we describe an improved algorithm for contraction of matchgate networks on non-planar graphs. Let Σ be a standard oriented closed surface of genus g , i.e., a sphere with g handles.

DEFINITION 1. *Given a graph $G = (V, E)$ embedded into a surface Σ we shall say that G is contractible if there exists a region $D \subset \Sigma$ with topology of a disk containing all vertices and all edges of G . A subset of edges $M \subseteq E$ is called a planar cut of G if a graph $G_M = (V, E \setminus M)$ is contractible.*

A contraction value $c(\mathcal{T})$ of a tensor network \mathcal{T} is a complex number obtained by contracting all tensors of \mathcal{T} . Our main result is as follows.

THEOREM 1. *Let \mathcal{T} be a matchgate tensor network on a graph $G = (V, E)$ with n vertices embedded into a surface of genus g . Assume we are given a planar cut of G with m edges. Then the contraction value $c(\mathcal{T})$ can be computed in time $T = O((n+m)^6) + O(m^3) 2^{2g}$. If G has a bounded vertex degree, one can compute $c(\mathcal{T})$ in time $T = O((n+m)^3) + O(m^3) 2^{2g}$.*

If a network has a small planar cut, $m \ll n$, the theorem provides a speedup for computing the matching sum and the partition function of the Ising model compared to the FKT method. For example, computing the matching sum of a graph G as above by the FKT method would require time $T = O(n^3) 2^{2g}$ since the matching sum is expressed as a linear combination of 2^{2g} Pfaffians where each Pfaffian involves a matrix of size $n \times n$, see [11, 12, 13], and since Pfaffian of an $n \times n$ matrix can be computed in time $O(n^3)$, see Section 2.2. In contrast to the FKT method, our algorithm is divided into two stages. At the first stage that requires time $O((n+m)^6)$ one performs a partial contraction of the planar subgraph G_M determined by the given planar cut M , see Def. 1. The contraction reduces the number of edges in a network down to m without changing the genus². The first stage of the algorithm yields a new network \mathcal{T}' with a single vertex and m self-loops such that $c(\mathcal{T}') = c(\mathcal{T})$. At the second stage one contracts the network \mathcal{T}' by expressing the contraction value $c(\mathcal{T}')$ as a linear combination of 2^{2g} Pfaffians similar to the FKT method. However each Pfaffian involves a matrix of size only $O(m) \times O(m)$.

Remark 1: The statement of the theorem assumes that all tensors are specified by their generating functions, see Section 3 for details. It allows one to describe a matchgate tensor of rank d using only $O(d^2)$ parameters. We also assume that the ordering of indexes in any tensor is consistent with the orientation of a surface. See Section 2.1 for a formal definition of tensor networks.

2. Some definitions and notations

2.1. Tensor networks. Throughout this paper a tensor of rank d is a d -dimensional complex array T in which the indexes take values 0 and 1. Given a binary string of indexes $x = (x_1 x_2 \dots x_d)$ we shall denote the corresponding component $T_{x_1 x_2 \dots x_d}$ as $T(x)$.

²If the initial network represents a matchings sum, the first stage of the algorithm would require only time $O((n+m)^3)$.

A tensor network is a product of tensors whose indexes are pairwise contracted. More specifically, each tensor is represented by a vertex of some graph $G = (V, E)$, where V is a set of vertices and E is a set of edges. The graph may have self-loops and multiple edges. For every edge $e \in E$ one defines a variable $x(e)$ taking values 0 and 1. A bit string x that assigns a particular value to every variable $x(e)$ is called an *index string*. A set of all possible index strings will be denoted $\mathcal{X}(E)$. In order to define a tensor network on G one has to order edges incident to every vertex. We shall assume that G is specified by its *incidence list*, i.e., for every vertex u one specifies an ordered list of edges incident to u which will be denoted $E(u)$. Thus $E(u) = \{e_1^u, \dots, e_{d(u)}^u\}$ where $e_j^u \in E$ for all j . Here $d(u) = |E(u)|$ is the degree of u . If a vertex u has one or several self-loops, we assume that every self-loop appears in the list $E(u)$ twice (because it will represent contraction of two indexes). For example, a vertex with one self-loop and no other incident edges has degree 2. A tensor network on G is a collection of tensors $\mathcal{T} = \{T_u\}_{u \in V}$ labeled by vertices of G such that a tensor T_u has rank $d(u)$. A *contraction value* of a network \mathcal{T} is defined as

$$(3) \quad c(\mathcal{T}) = \sum_{x \in \mathcal{X}(E)} \prod_{u \in V} T_u(x(e_1^u) \dots x(e_{d(u)}^u)).$$

Thus the contraction value can be computed by taking a tensor product of all tensors $\{T_u\}$ and then contracting those pairs of indexes that correspond to the same edge of the graph. By definition, $c(\mathcal{T})$ is a complex number (tensor of rank 0).

It will be implicitly assumed throughout this paper that a tensor network is defined on a graph G embedded into a closed oriented surface Σ . We require that the order of edges incident to any vertex u must agree with the order in which the edges appear if one circumnavigates u counterclockwise. Thus the order on any set $E(u)$ is completely specified by the choice of the first edge $e_1^u \in E(u)$. If the surface Σ has genus g we shall say that G has genus g (it may or may not be the minimal genus for which the embedding of G into Σ is possible).

2.2. Pfaffian — basis facts. Recall that Pfaffian of an $n \times n$ antisymmetric matrix A is defined as

$$\text{Pf}(A) = \frac{1}{2^m m!} \sum_{\sigma \in S_n} \text{sgn}(\sigma) A_{\sigma(1), \sigma(2)} A_{\sigma(3), \sigma(4)} \cdots A_{\sigma(n-1), \sigma(n)}$$

if $n = 2m$ is even, and $\text{Pf}(A) = 0$ if n is odd. Here S_n is the symmetric group and $\text{sgn}(\sigma) = \pm 1$ is the parity of a permutation σ . One can efficiently compute Pfaffian up to a sign using an identity $\text{Pf}(A)^2 = \det(A)$. However, in order to compute a linear combination of several Pfaffians one needs to know the sign exactly. One can directly compute $\text{Pf}(A)$ using the combinatorial algorithm by Mahajan et al [20] in time $O(n^4)$. Alternatively, one can use Gaussian elimination to find an invertible matrix U such that $U^T A U$ is block-diagonal with all blocks of size 2×2 . It requires time $O(n^3)$. Then $\text{Pf}(A)$ can be computed using an identity $\text{Pf}(U A U^T) = \det(U) \text{Pf}(A)$. This method yields $O(n^3)$ algorithm although it is less computationally stable compared to the combinatorial algorithm of [20].

2.3. Anticommuting variables. In this section we introduce notations pertaining to the Grassmann algebra and anticommuting variables (see, for instance,

a textbook [21]). Consider a set of formal variables $\theta = (\theta_1, \dots, \theta_n)$ subject to multiplication rules

$$(4) \quad \theta_a^2 = 0, \quad \theta_a \theta_b + \theta_b \theta_a = 0 \quad \text{for all } a, b.$$

The Grassmann algebra $\mathcal{G}(\theta)$ is the algebra of complex polynomials in variables $\theta_1, \dots, \theta_n$ factorized over the ideal generated by Eq. (4). Equivalently, $\mathcal{G}(\theta)$ is the exterior algebra of the vector space \mathbb{C}^n , where each variable θ_a is regarded as a basis vector of \mathbb{C}^n . More generally, the variables θ_a may be labeled by elements of an arbitrary finite set X (in our case the variables will be associated with edges or vertices of a graph). A linear basis of $\mathcal{G}(\theta)$ is spanned by 2^n monomials in variables θ_a . Namely, for any subset $M \subseteq \{1, \dots, n\}$ define a *normally ordered* monomial

$$(5) \quad \theta(M) = \prod_{a \in M} \theta_a$$

where the indexes increase from the left to the right. If the variables are labeled by elements of some set X , one can define the normally ordered monomials $\theta(M)$, $M \subseteq X$ by choosing some order on X . Let us agree that $\theta(\emptyset) = I$. Then an arbitrary element $f \in \mathcal{G}(\theta)$ can be written as

$$(6) \quad f = \sum_{M \subseteq \{1, \dots, n\}} f(M) \theta(M), \quad f(M) \in \mathbb{C}.$$

We shall use notations f and $f(\theta)$ interchangeably meaning that f can be regarded as a function of anticommuting variables $\theta = (\theta_1, \dots, \theta_n)$. Accordingly, elements of the Grassmann algebra will be referred to as functions. In particular, I is regarded as a constant function. A function $f(\theta)$ is called even (odd) if it is a linear combination of monomials $\theta(M)$ with even (odd) degree. Even functions span the central subalgebra of $\mathcal{G}(\theta)$.

We shall often consider several species of Grassmann variables, for example, $\theta = (\theta_1, \dots, \theta_n)$ and $\eta = (\eta_1, \dots, \eta_k)$. It is always understood that different variables anticommute. For example, a function $f(\theta, \eta)$ must be regarded as an element of the Grassmann algebra $\mathcal{G}(\theta, \eta)$, that is, a linear combination of monomials in $\theta_1, \dots, \theta_n$ and η_1, \dots, η_k .

A partial derivative over a variable θ_a is a linear map $\partial_a : \mathcal{G}(\theta) \rightarrow \mathcal{G}(\theta)$ defined by requirement $\partial_a \cdot I = 0$ and the Leibniz rule

$$\partial_a \cdot (\theta_b f) = \delta_{a,b} f - \theta_b (\partial_a \cdot f).$$

More explicitly, given any function $f \in \mathcal{G}(\theta)$, represent it as $f(\theta) = f_0 + \theta_a f_1$, where $f_0, f_1 \in \mathcal{G}(\theta)$ do not depend on θ_a . Then $\partial_a f = f_1$. It follows that $\partial_a \cdot \theta_a = I$, $\partial_a \theta_b = -\theta_b \partial_a$, $\partial_a \partial_b = -\partial_b \partial_a$ for $a \neq b$ and $\partial_a^2 = 0$.

A linear change of variables $\theta_a = \sum_{b=1}^n U_{a,b} \tilde{\theta}_b$ with an invertible matrix U induces an automorphism of the algebra $\mathcal{G}(\theta)$ such that $f(\theta) \rightarrow f(\tilde{\theta})$. The corresponding transformation of partial derivatives is

$$(7) \quad \partial_a = \sum_{b=1}^n (U^{-1})_{b,a} \tilde{\partial}_b.$$

2.4. Gaussian integrals. Let $\theta = (\theta_1, \dots, \theta_n)$ be a set of Grassmann variables. An integral over a variable θ_a denoted by $\int d\theta_a$ is a linear map from $\mathcal{G}(\theta_1, \dots, \theta_n)$ to $\mathcal{G}(\theta_1, \dots, \hat{\theta}_a, \dots, \theta_n)$, where $\hat{\theta}_a$ means that the variable θ_a is omitted. To define an integral $\int d\theta_a f(\theta)$, represent the function f as $f = f_0 + \theta_a f_1$,

where $f_0, f_1 \in \mathcal{G}(\theta_1, \dots, \hat{\theta}_a, \dots, \theta_n)$. Then $\int d\theta_a f(\theta) = f_1$. Thus one can compute the integral $\int d\theta_a f(\theta)$ by first computing the derivative $\partial_a \cdot f(\theta)$ and then excluding the variable θ_a from the list of variables of f .

Given an ordered set of Grassmann variables $\theta = (\theta_1, \dots, \theta_n)$ we shall use a shorthand notation

$$\int D\theta = \int d\theta_n \cdots \int d\theta_2 \int d\theta_1.$$

Thus $\int D\theta$ can be regarded as a linear functional on $\mathcal{G}(\theta)$, or as a linear map from $\mathcal{G}(\theta, \eta)$ to $\mathcal{G}(\eta)$, and so on. The action of $\int D\theta$ on the normally ordered monomials is as follows

$$(8) \quad \int D\theta \theta(M) = \begin{cases} 1 & \text{if } M = \{1, 2, \dots, n\}, \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, if one regards $\int D\theta$ as a linear map from $\mathcal{G}(\theta, \eta)$ to $\mathcal{G}(\eta)$ then

$$\int D\theta \theta(M) \eta(K) = \begin{cases} \eta(K) & \text{if } M = \{1, 2, \dots, n\}, \\ 0 & \text{otherwise.} \end{cases}$$

Although this definition assumes that both variables θ, η have a normal ordering, the integral $\int D\theta$ depends only on the ordering of θ .

One can easily check that integrals over different variables anticommute. More generally, if $\theta = (\theta_1, \dots, \theta_n)$ and $\eta = (\eta_1, \dots, \eta_k)$ then

$$(9) \quad \int D\theta \int D\eta = (-1)^{nk} \int D\eta \int D\theta.$$

Under a linear change of variables $\theta_a = \sum_{b=1}^n U_{a,b} \eta_b$ the integral transforms as

$$(10) \quad \int D\theta = \det(U) \int D\eta.$$

In the rest of the section we consider two species of Grassmann variables $\theta = (\theta_1, \dots, \theta_n)$ and $\eta = (\eta_1, \dots, \eta_k)$. Given an antisymmetric $n \times n$ matrix A and any $n \times k$ matrix B , define quadratic forms

$$\theta^T A \theta = \sum_{a,b=1}^n A_{a,b} \theta_a \theta_b, \quad \theta^T B \eta = \sum_{a=1}^n \sum_{b=1}^k B_{a,b} \theta_a \eta_b.$$

Gaussian integrals over Grassmann variables are defined as follows.

$$(11) \quad I(A) \stackrel{\text{def}}{=} \int D\theta \exp\left(\frac{1}{2} \theta^T A \theta\right) \quad \text{and} \quad I(A, B) \stackrel{\text{def}}{=} \int D\theta \exp\left(\frac{1}{2} \theta^T A \theta + \theta^T B \eta\right).$$

Thus $I(A)$ is just a complex number while $I(A, B)$ is an element of $\mathcal{G}(\eta)$. Below we present the standard formulas for the Gaussian integrals. Firstly,

$$(12) \quad I(A) = \text{Pf}(A).$$

Secondly, if A is an invertible matrix then

$$(13) \quad I(A, B) = \text{Pf}(A) \exp\left(\frac{1}{2} \eta^T B^T A^{-1} B \eta\right).$$

Assume now that A has rank m for some even³ integer $0 \leq m \leq n$. Choose any invertible matrix U such that AU has zero columns $m+1, \dots, n$. (This is equivalent

³Note that antisymmetric matrices always have even rank.

to finding a basis of \mathbb{C}^n such that the last $n - m$ basis vectors belong to the zero subspace of A .) Then

$$U^T A U = \begin{bmatrix} A_{11} & 0 \\ 0 & 0 \end{bmatrix},$$

for some invertible $m \times m$ matrix A_{11} . Introduce also matrices B_1, B_2 of size $m \times k$ and $(n - m) \times k$ respectively such that

$$U^T B = \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}.$$

Performing a change of variables $\theta = U\tilde{\theta}$ in Eq. (11) and introducing variables $\tau = (\tau_1, \dots, \tau_m)$ and $\mu = (\mu_1, \dots, \mu_{n-m})$ such that $\tilde{\theta} = (\tau, \mu)$ one gets

$$I(A, B) = \det(U) \int D\tau \exp\left(\frac{1}{2} \tau^T A_{11} \tau + \tau^T B_1 \eta\right) \int D\mu \exp(\mu^T B_2 \eta).$$

Here we have taken into account Eqs. (9,10). Applying Eq. (13) to the first integral one gets

$$(14) \quad I(A, B) = \text{Pf}(A_{11}) \det(U) \exp\left(\frac{1}{2} \eta^T B_1^T (A_{11})^{-1} B_1 \eta\right) \int D\mu \exp(\mu^T B_2 \eta).$$

One can easily check that $\int D\mu \exp(\mu^T B_2 \eta) = 0$ if the rank of B_2 is smaller than the number of variables in μ , that is, $n - m$. Since B_2 has only k columns we conclude that

$$I(A, B) = 0 \quad \text{unless} \quad m \geq n - k.$$

Therefore in the non-trivial case $I(A, B) \neq 0$ the matrices $B_1^T (A_{11})^{-1} B_1$ and B_2 specifying $I(A, B)$ have size $k \times k$ and $k' \times k$ for some $k' \leq k$. It means that $I(A, B)$ can be specified by $O(k^2)$ bits. One can compute $I(A, B)$ in time $O(n^3 + n^2 k)$. Indeed, one can use Gaussian elimination to find U , compute $\det(U)$ and $\text{Pf}(A_{11})$ in time $O(n^3)$. The matrix A_{11}^{-1} can be computed in time $O(n^3)$. Computing the matrices B_1, B_2 requires time $O(n^2 k)$.

The formula Eq. (14) will be our main tool for contraction of matchgate tensor networks.

3. Matchgate tensors

3.1. Basic properties of matchgate tensors. Although the definition of a matchgate tensor in terms of the matchgate identities Eq. (1) is very simple, it is neither very insightful nor very useful. Two equivalent but more operational definitions will be given in Sections 3.3, 3.4. Here we list some basic properties of matchgate tensors that can be derived directly from Eq. (1). In particular, following the approach of [17], we prove that a matchgate tensor of rank n can be specified by a *mean vector* $z \in \{0, 1\}^n$ and a *covariance matrix* A of size $n \times n$.

PROPOSITION 1. *Let T be a matchgate tensor of rank n . For any $z \in \{0, 1\}^n$ a tensor T' with components $T'(x) = T(x \oplus z)$ is a matchgate tensor.*

PROOF. Indeed, make a change of variables $x \rightarrow x \oplus z$, $y \rightarrow y \oplus z$ in the matchgate identities □

Let T be a non-zero matchgate tensor of rank n . Choose any string z such that $T(z) \neq 0$ and define a new tensor T' with components

$$T'(x) = \frac{T(x \oplus z)}{T(z)}, \quad x \in \{0, 1\}^n,$$

such that T' is a matchgate and $T'(0^n) = 1$. Introduce an antisymmetric $n \times n$ matrix A such that

$$A_{a,b} = \begin{cases} T'(e^a \oplus e^b) & \text{if } a < b, \\ -T'(e^a \oplus e^b) & \text{if } a > b, \\ 0 & \text{if } a = b. \end{cases}$$

PROPOSITION 2. *For any $x \in \{0, 1\}^n$*

$$T'(x) = \begin{cases} \text{Pf}(A(x)) & \text{if } x \text{ has even weight} \\ 0 & \text{if } x \text{ has odd weight} \end{cases},$$

where $A(x)$ is a matrix obtained from A by removing all rows and columns a such that $x_a = 0$.

PROOF. Let us prove the proposition by induction in the weight of x . Choosing $x = 0^n$ and $y = e^a$ in the matchgate identities Eq. (1) one gets $T'(e^a) = 0$ for all a . Similarly, choosing $x = e^b$ and $y = e^a$ with $a < b$ one gets $T'(e^a \oplus e^b) = A_{a,b} = \text{Pf}(A(e^a \oplus e^b))$. Thus the proposition is true for $|x| = 1, 2$. Assume it is true for all strings x of weight $\leq k$. For any string x of weight $k+1$ and any a such that $x_a = 0$ apply the matchgate identities Eq. (1) with x and $y = e^a$. After simple algebra one gets

$$T'(x \oplus e^a) = \sum_{b: x_b=1} A_{a,b} T'(x \oplus e^b) (-1)^{\eta(a,b)}, \quad \eta(a,b) = \sum_{j=a}^{b-1} x_j.$$

Noting that $x \oplus e^b$ has weight k and applying the induction hypothesis one gets

$$T'(x \oplus e^a) = \sum_{b: x_b=1} A_{a,b} \text{Pf}(A(x \oplus e^b)) (-1)^{\eta(a,b)}$$

for even k and $T'(x \oplus e^a) = 0$ for odd k . Thus $T'(y) = 0$ for all odd strings of weight $k+2$. Furthermore, let non-zero bits of $x \oplus e^b$ be located at positions $j_1 < j_2 < \dots < j_k$. Note that the sign of $A_{a,b} (-1)^{\eta(a,b)}$ coincides with the parity of a permutation that orders elements in a set $[a, b, j_1, j_2, \dots, j_k]$. Therefore, by definition of Pfaffian one gets $T'(x \oplus e^a) = \text{Pf}(A(x \oplus e^a))$. \square

Thus one can regard the vector z and the matrix A above as analogues of a mean vector and a covariance matrix for Gaussian states of fermionic modes, see for instance [19]. Although Proposition 2 provides a concise description of a matchgate tensor, it is not very convenient for contracting matchgate networks because the mean vector z and the covariance matrix A are not uniquely defined.

COROLLARY 1. *Any matchgate tensor is either even or odd.*

PROOF. Indeed, the proposition above implies that if a matchgate tensor T has even (odd) mean vector it is an even (odd) tensor. \square

3.2. Describing a tensor by a generating function. Let $\theta = (\theta_1, \dots, \theta_n)$ be an ordered set of n Grassmann variables. For any tensor T of rank n define a generating function $T \in \mathcal{G}(\theta)$ according to

$$T(\theta) = \sum_{x \in \{0,1\}^n} T(x) \theta(x).$$

Here $\theta(x) = \theta_1^{x_1} \cdots \theta_n^{x_n}$ is the normally ordered monomial corresponding to the subset of indexes $x = \{a : x_a = 1\}$. Let us introduce a linear differential operator Λ acting on the tensor product of two Grassmann algebras $\mathcal{G}(\theta) \otimes \mathcal{G}(\theta)$ such that

$$(15) \quad \Lambda = \sum_{a=1}^n \theta_a \otimes \partial_a + \partial_a \otimes \theta_a.$$

LEMMA 1. *A tensor T of rank n is a matchgate iff*

$$(16) \quad \Lambda \cdot T \otimes T = 0.$$

PROOF. Denote $\Lambda_a = \theta_a \otimes \partial_a + \partial_a \otimes \theta_a$. For any strings $x, y \in \{0,1\}^n$ one has the following identity:

$$\Lambda_a \cdot \theta(x) \otimes \theta(y) = \begin{cases} 0 & \text{if } x_a = y_a, \\ (-1)^{x_1 + \dots + x_{a-1} + y_1 + \dots + y_{a-1}} \theta(x \oplus e_a) \otimes \theta(y \oplus e_a) & \text{if } x_a \neq y_a. \end{cases}$$

Expanding both factors T in Eq. (16) in the monomials $\theta(x), \theta(y)$, using the above identity, and performing a change of variable $x \rightarrow x \oplus e_a$ and $y \rightarrow y \oplus e_a$ for every a one gets a linear combination of monomials $\theta(x) \otimes \theta(y)$ with the coefficients given by the right hand side of Eq. (1). Therefore Eq. (16) is equivalent to Eq. (1). \square

Lemma 1 provides an alternative definition of a matchgate tensor which is much more useful than the original definition Eq. (1). For example, it is shown below that the operator Λ has a lot of symmetries which can be translated into a group of transformations preserving the subset of matchgate tensors.

LEMMA 2. *The operator Λ is invariant under linear reversible changes of variables $\theta_a = \sum_{b=1}^n U_{a,b} \tilde{\theta}_b$.*

PROOF. Indeed, let $\tilde{\partial}_a$ be the partial derivative over $\tilde{\theta}_a$. Using Eq. (7) one gets

$$\sum_{a=1}^n \theta_a \otimes \partial_a + \partial_a \otimes \theta_a = \sum_{a,b,c=1}^n U_{a,b} (U^{-1})_{c,a} (\tilde{\theta}_b \otimes \tilde{\partial}_c + \tilde{\partial}_c \otimes \tilde{\theta}_b) = \sum_b (\tilde{\theta}_b \otimes \tilde{\partial}_b + \tilde{\partial}_b \otimes \tilde{\theta}_b).$$

\square

Lemmas 1,2 imply that linear reversible change of variables $T(\theta) \rightarrow T(\tilde{\theta})$, where $\theta_a = \sum_{b=1}^n U_{a,b} \tilde{\theta}_b$ map matchgates to matchgates.

COROLLARY 2. *Let T be a matchgate tensor of rank n . Then a tensor T' defined by any of the following transformations is also a matchgate.*

- (Cyclic shift): $T'(x_1, x_2, \dots, x_n) = T(x_2, \dots, x_n, x_1)$,
- (Reflection): $T'(x_1, x_2, \dots, x_n) = T(x_n, \dots, x_2, x_1)$,
- (Phase shift): $T'(x) = (-1)^{x \cdot z} T(x)$, where $z \in \{0,1\}^n$.

PROOF. Let $\epsilon = 0$ if T is an even tensor and $\epsilon = 1$ if T is an odd tensor, see Corollary 1. The transformations listed above are generated by the following linear changes of variables:

$$\begin{aligned} \text{Phase shift} &: \theta_a \rightarrow (-1)^{z_a} \theta_a, \quad a = 1, \dots, n. \\ \text{Cyclic shift} &: \theta_a \rightarrow \theta_{a-1} \quad a = 2, \dots, n, \quad \text{and} \quad \theta_1 \rightarrow (-1)^{\epsilon+1} \theta_n. \\ \text{Reflection} &: \theta_a \rightarrow i \theta_{n-a}. \end{aligned}$$

Indeed, let $\theta(x)$ be the normally ordered monomial where $x = (x_1, x_2, \dots, x_n)$. Let $x' = (x_2, \dots, x_n, x_1)$ for the cyclic shift and $x' = (x_n, \dots, x_2, x_1)$ for the reflection. Then the linear changes of variables stated above map $\theta(x)$ to $(-1)^{z \cdot x} \theta(x)$ for the phase shift, to $\theta(x')$ for the cyclic shift, and to $i^\epsilon \theta(x')$ for the reflection. Therefore, in all three cases T' is a matchgate tensor. \square

3.3. Matchgate tensors have Gaussian generating function. A memory size required to store a tensor of rank n typically grows exponentially with n . However the following theorem shows that for matchgate tensors the situation is much better.

THEOREM 2. *A tensor T of rank n is a matchgate iff there exist an integer $0 \leq k \leq n$, complex matrices A, B of size $n \times n$ and $k \times n$ respectively, and a complex number C such that T has generating function*

$$(17) \quad T(\theta) = C \exp\left(\frac{1}{2} \theta^T A \theta\right) \int D\mu \exp(\mu^T B \theta),$$

where $\mu = (\mu_1, \dots, \mu_k)$ is a set of k Grassmann variables. Furthermore, one can always choose the matrices A and B such that $A^T = -A$ and $BA = 0$.

Thus the triple (A, B, C) provides a concise description of a matchgate tensor that requires a memory size only $O(n^2)$. In addition, it will be shown that contraction of matchgate tensors can be efficiently implemented using the representation Eq. (17) and the Gaussian integral formulas of Section 2.4. We shall refer to the generating function Eq. (17) as a *canonical generating function* for a matchgate tensor T .

COROLLARY 3. *For any matrices A and B the Gaussian integral $I(A, B)$ defined in Eq. (11) is a matchgate.*

PROOF. Indeed, use Eq. (14) and Theorem 2. \square

In the rest of the section we shall prove Theorem 2.

PROOF OF THEOREM 2. Let us first verify that the tensor defined in Eq. (17) is a matchgate, i.e., $\Lambda \cdot T \otimes T = 0$, see Lemma 1. Without loss of generality A is an antisymmetric matrix and $C = 1$. Write T as

$$T = T_2 T_1, \quad \text{where} \quad T_2 = \exp\left(\frac{1}{2} \theta^T A \theta\right), \quad T_1 = \int D\mu \exp(\mu^T B \theta).$$

Noting that T_2 is an even function and $\partial_a \theta(x) = \partial_a \cdot \theta(x) + \theta(x) \partial_a$ for any even string x one concludes that

$$(18) \quad \Lambda \cdot T \otimes T = (\Lambda \cdot T_2 \otimes T_2) T_1 \otimes T_1 + T_2 \otimes T_2 (\Lambda \cdot T_1 \otimes T_1).$$

Therefore it suffices to prove that $\Lambda \cdot T_2 \otimes T_2 = 0$ and $\Lambda \cdot T_1 \otimes T_1 = 0$. The first identity follows from $\partial_a \cdot T_2 = \sum_{b=1}^n A_{a,b} \theta_b T_2$ and $A^T = -A$ which implies

$$\Lambda \cdot T_2 \otimes T_2 = \sum_{a,b=1}^n A_{a,b} (\theta_a \otimes \theta_b + \theta_b \otimes \theta_a) T_2 \otimes T_2 = 0.$$

To prove the second identity consider the singular value decomposition $B = L^T \tilde{B} R$, where $L \in SU(k)$ and $R \in SU(n)$ are unitary operators, while \tilde{B} is a $k \times n$ matrix with all non-zero elements located on the main diagonal, $\tilde{B} = \text{diag}(B_1, \dots, B_k)$. Introducing new variables $\tilde{\theta} = R \theta$ and $\tilde{\mu} = L \mu$ one gets

$$T_1 = \int D\tilde{\mu} \exp \left(\sum_{a=1}^k B_a \tilde{\mu}_a \tilde{\theta}_a \right) = B_1 \cdots B_k \tilde{\theta}_1 \cdots \tilde{\theta}_k.$$

Here we have used identity $\int D\tilde{\mu} = \det(L) \int D\mu = \int D\mu$, see Eq. (10). Since Λ is invariant under linear reversible changes of variables, see Lemma 2, and since $\Lambda \cdot \theta(x) \otimes \theta(x) = 0$ for any monomial $\theta(x)$ one gets $\Lambda \cdot T_1 \otimes T_1 = 0$. We proved that $\Lambda \cdot T \otimes T = 0$, that is, T is a matchgate tensor.

Let us now show that any matchgate tensor T of rank n can be written as in Eq. (17). Define a linear subspace $\mathcal{Z} \subseteq \mathbb{C}^n$ such that

$$\mathcal{Z} = \left\{ \xi \in \mathbb{C}^n : \sum_{a=1}^n \xi_a \theta_a T = 0 \right\}.$$

Let $\dim(\mathcal{Z}) = k$. Make a change of variables $\eta = U \theta$ where U is any invertible matrix such that the last k rows of U span \mathcal{Z} . Then $\eta_a T = 0$ for all $a = n - k + 1, \dots, n$. It follows that T can be represented as

$$(19) \quad T = \eta_{n-k+1} \cdots \eta_n S$$

for some function $S = S(\eta)$ that depends only on variables $\eta_1, \dots, \eta_{n-k}$. Equivalently,

$$S = \partial_n \cdots \partial_{n-k+1} \cdot T,$$

where the partial derivatives are taken with respect to the variables η . Since Λ is invariant under reversible linear changes of variables, see Lemma 2, and since $\Lambda \partial_a \otimes \partial_a = \partial_a \otimes \partial_a \Lambda$, we get

$$(20) \quad \Lambda \cdot S \otimes S = \sum_{a=1}^{n-k} \eta_a S \otimes \partial_a \cdot S + \partial_a \cdot S \otimes \eta_a S = 0.$$

By definition of the subspace \mathcal{Z} the functions $\eta_1 S, \dots, \eta_{n-k} S$ are linearly independent. Therefore there exist linear functionals $F_a : \mathcal{G}(\eta) \rightarrow \mathbb{C}$, $a = 1, \dots, n - k$, such that $F_a(\eta_b S) = \delta_{a,b}$. Applying F_a to the first factor in Eq. (20) we get

$$(21) \quad \partial_a \cdot S = \sum_{b=1}^{n-k} M_{a,b} \eta_b S, \quad \text{where} \quad M_{a,b} = -F_a(\partial_b \cdot S) \in \mathbb{C},$$

for all $a = 1, \dots, n - k$. Let k_{\min} the lowest degree of monomials in S . Let us show that $k_{\min} = 0$, that is, $S(\eta)$ contains I with a non-zero coefficient. Indeed, let S_{\min} be a function obtained from S by retaining only monomials of degree k_{\min} . Since any monomial in the r.h.s. of Eq. (21) has degree at least $k_{\min} + 1$, we conclude that $\partial_a \cdot S_{\min} = 0$ for all a . It means that $S_{\min} = C I$ for some complex number $C \neq 0$ and thus $k_{\min} = 0$.

Applying the partial derivative ∂_b to Eq. (21) we get $M_{a,b} = C^{-1}(\partial_b \partial_a \cdot S)|_{\eta=0}$, where the substitution $\eta = 0$ means that the term proportional to the identity is taken. Since the partial derivatives over different variables anticommute, M is an antisymmetric matrix.

Using Gaussian elimination any antisymmetric matrix M can be brought into a block-diagonal form with 2×2 blocks on the diagonal by a transformation $M \rightarrow M' = W^T X W$, where W is an invertible matrix (in fact, one can always choose unitary W , see [23]). Since our change of variables $\eta = U\theta$ allows arbitrary transformations in the subspace of $\eta_1, \dots, \eta_{n-k}$ we can assume that M is already block-diagonal,

$$M = \bigoplus_{a=1}^m \begin{pmatrix} 0 & \lambda_a \\ -\lambda_a & 0 \end{pmatrix}, \quad \lambda_1, \dots, \lambda_m \in \mathbb{C},$$

where only non-zero blocks are represented, so that $2m \leq n - k$.

Applying Eq. (21) for $a = 1, 2$ we get

$$(22) \quad \partial_1 \cdot S = \lambda_1 \eta_2 S, \quad \partial_2 \cdot S = -\lambda_1 \eta_1 S.$$

Note that S can be written as

$$(23) \quad S = \sum_x (\alpha_x \eta_1 + \beta_x \eta_2) \eta(x) + \sum_y (\gamma_y I + \delta_y \eta_1 \eta_2) \eta(y),$$

where the sums over x and y run over all odd and even monomials in $\eta_3, \dots, \eta_{n-k}$ respectively. Substituting Eq. (23) into Eq. (22) one gets $\alpha_x = \beta_x = 0$ and $\delta_x = \lambda_1 \gamma_x$, that is

$$S = (I + \lambda_1 \eta_1 \eta_2) S',$$

where S' depends only on variables $\eta_3, \dots, \eta_{n-k}$. Repeating this argument inductively, we arrive to the representation

$$S = C \prod_{a=1}^m (I + \lambda_a \eta_{2a-1} \eta_{2a}) = C \exp \left(\frac{1}{2} \eta^T M \eta \right).$$

Here we extended the matrix M such that its last k columns and rows are zero. Combining it with Eq. (19) one gets

$$T = C \eta_{n-k+1} \cdots \eta_n \exp \left(\frac{1}{2} \eta^T M \eta \right) = C \exp \left(\frac{1}{2} \eta^T M \eta \right) \int D\mu \exp \left(\mu^T \tilde{B} \eta \right),$$

where μ is a vector of k Grassmann variables and \tilde{B} is a $k \times n$ matrix with 0,1 entries such that

$$\mu^T \tilde{B} \eta = \sum_{a=1}^k \mu_a \eta_{n-k+a}.$$

Recalling that $\eta = U\theta$, we conclude that T has a representation Eq. (17) with $A = U^T M U$ and $B = \tilde{B} U$. As a byproduct we also proved that the matrices A , B in Eq. (17) can always be chosen such that $BA = 0$ since $BA = \tilde{B} M U$ and all non-zero entries of \tilde{B} are in the last k rows. \square

3.4. Graph theoretic definition of matchgate tensors. Let $G = (V, E, W)$ be an arbitrary weighted graph with a set of vertices V , set of edges E and a weight function W that assigns a complex weight $W(e)$ to every edge $e \in E$.

DEFINITION 2. Let $G = (V, E)$ be a graph and $S \subseteq V$ be a subset of vertices. A subset of edges $M \subseteq E$ is called an S -imperfect matching iff every vertex from S has no incident edges from M while every vertex from $V \setminus S$ has exactly one incident edge from M . A set of all S -imperfect matchings in a graph G will be denoted $\mathcal{M}(G, S)$.

Note that a perfect matching corresponds to an \emptyset -imperfect matching. Occasionally we shall denote a set of perfect matching by $\mathcal{M}(G) \equiv \mathcal{M}(G, \emptyset)$. For any subset of vertices $S \subseteq V$ define a *matching sum*

$$(24) \quad \text{PerfMatch}(G, S) = \sum_{M \in \mathcal{M}(G, S)} \prod_{e \in M} W(e).$$

(A matching sum can be identified with a planar matchgate of [15].) In this section we outline an isomorphism between matchgate tensors and matching sums of planar graphs discovered earlier in [18]. For the sake of completeness we provide a proof of this result below. Although the main idea of the proof is the same as in [18] some technical details are different. In particular, we use much simpler crossing gadget.

Specifically, we shall consider planar weighted graphs $G = (V, E, W)$ embedded into a disk such that some subset of n *external* vertices $V_{\text{ext}} \subseteq V$ belongs to the boundary of disk while all other *internal* vertices $V \setminus V_{\text{ext}}$ belong to the interior of D . Let $V_{\text{ext}} = \{u_1, \dots, u_n\}$ be an ordered list of external vertices corresponding to circumnavigating anticlockwise the boundary of the disk. Then any binary string $x \in \{0, 1\}^n$ can be identified with a subset $x \subseteq V_{\text{ext}}$ that includes all external vertices u_j such that $x_j = 1$. Now we are ready to state the main result of this section.

THEOREM 3. For any matchgate tensor T of rank n there exists a planar weighted graph $G = (V, E, W)$ with $O(n^2)$ vertices, $O(n^2)$ edges and a subset of n vertices $V_{\text{ext}} \subseteq V$ such that

$$(25) \quad T(x) = \text{PerfMatch}(G, x) \quad \text{for all } x \subseteq V_{\text{ext}}.$$

Furthermore, suppose $T = C \exp\left(\frac{1}{2} \theta^T A \theta\right) \int D\mu \exp(\mu^T B \theta)$ is a generating function of T . Given A , B , and C the graph G can be constructed in time $O(n^2)$ and the weights $W(e)$ are linear functionals of A , B , and C .

The key step in proving the theorem is to show that Pfaffian of any $n \times n$ antisymmetric matrix can be expressed as a matching sum on some planar graph with $O(n^2)$ vertices. This step can be regarded as a reversal of the FKT method that allows one to represent the matching sum of a planar graph as Pfaffian of the Tutte matrix.

LEMMA 3. For any complex antisymmetric matrix A of size $n \times n$ there exists a planar weighted graph $G = (V, E, W)$ with $O(n^2)$ vertices, $O(n^2)$ edges such that the weights $W(e)$ are linear functionals of A and

$$(26) \quad \text{Pf}(A) = \text{PerfMatch}(G, \emptyset).$$

The graph G can be constructed in time $O(n^2)$.

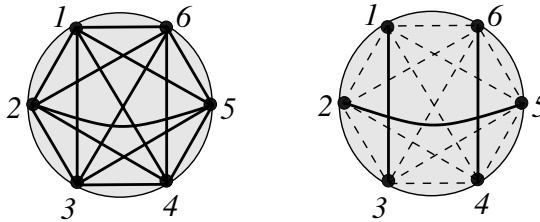


FIGURE 1. Left: a complete graph C_6 embedded into a disk. Right: a perfect matching on C_6 with two self-intersections.

Remark: It should be emphasized that we regard both sides of Eq. (26) as polynomial functions of matrix elements of A , and the lemma states that the two polynomials coincide. However, even if one treats both sides of Eq. (26) just as complex numbers, the statement of the lemma is still non-trivial, since one can not compute $\text{Pf}(A)$ in time $O(n^2)$ and thus one has to construct the graph G without access to the value of $\text{Pf}(A)$.

PROOF. Let us assume that n is even (otherwise the statement is trivial). Let D be a disk with n marked points v_1, \dots, v_n on the boundary such that their order corresponds to anticlockwise circumnavigating the boundary of D . Let C_n be the complete graph with vertices v_1, \dots, v_n embedded into D . We assume that the embedding is chosen such that all edges of C_n lie inside the disk and there are only double edge crossing points, see Fig. 1. Let $\mathcal{M}(C_n)$ be a set of perfect matchings on C_n . For any perfect matching $M \in \mathcal{M}(C_n)$ let $N_c(M)$ be the number of self-intersections in M , i.e., the number of edge crossing points in the planar embedding of C_n in which both crossing edges are occupied by M . For example, given a planar embedding of C_6 shown on Fig. 1, a perfect matching $M = (1, 3), (2, 5), (4, 6)$ has two self-intersections. We claim that

$$(27) \quad \text{Pf}(A) = \sum_{M \in \mathcal{M}(C_n)} (-1)^{N_c(M)} \prod_{(u,v) \in M, u < v} A_{u,v}.$$

Indeed, by definition of Pfaffian

$$(28) \quad \text{Pf}(A) = \sum_{\sigma} \text{sgn}(\sigma) A_{\sigma(1), \sigma(2)} \cdots A_{\sigma(n-1), \sigma(n)},$$

where the sum is over all permutations of n elements σ such that $\sigma(2j-1) < \sigma(2j)$ for all j and $\sigma(1) < \sigma(3) < \dots < \sigma(n-1)$. Clearly, there exists a one-to-one correspondence between such permutations and perfect matchings in C_n . If M is the perfect matching corresponding to the identity permutation, $M = (1, 2), \dots, (n-1, n)$, one has $N_c(M) = 0$ and the signs in Eqs. (27,28) coincide. Furthermore, changing M by any transposition $j \leftrightarrow j+1$ either does not change M or changes the parity of $N_c(M)$, so the signs in Eqs. (27,28) coincide for all perfect matchings.

In order to represent the sum over perfect matchings in Eq. (27) as a sum over perfect matchings in a planar graph we shall replace each edge crossing point of C_n by a *crossing gadget*, see Fig. 2. A *crossing gadget* is a planar simulator for an edge crossing point. It allows one to establish a correspondence between subsets of

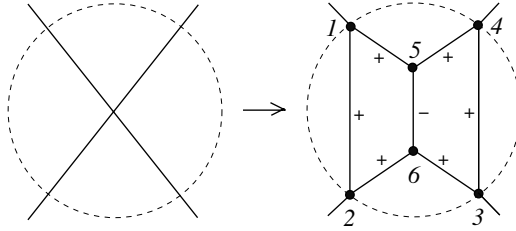


FIGURE 2. Each edge crossing point in the planar embedding of the complete graph C_n is replaced by the crossing gadget G_{cross} . Edges labeled by \pm carry a weight ± 1 .

edges in the non-planar graph and subsets of edges in a planar graph. In addition, a crossing gadget will take care of the extra sign⁴ factor in Eq. (27).

Crossing gadget. Consider a weighted graph G_{cross} shown on Fig. 2. It has 6 vertices and 7 edges. The edge (5,6) carries weight -1 and all other edges carry weight $+1$. We fix the embedding of G_{cross} into a disk such that G_{cross} has four external vertices $\{1, 2, 3, 4\}$ on the boundary of the disk. One can easily check that the matching sum of G_{cross} satisfies the following identities:

$$\begin{aligned} \text{PerfMatch}(G_{cross}, \emptyset) &= 1, \\ \text{PerfMatch}(G_{cross}, \{1, 3\}) &= \text{PerfMatch}(G_{cross}, \{2, 4\}) = 1, \\ \text{PerfMatch}(G_{cross}, \{1, 2, 3, 4\}) &= -1, \\ \text{PerfMatch}(G_{cross}, \{1, 2\}) &= \text{PerfMatch}(G_{cross}, \{3, 4\}) = 0, \\ \text{PerfMatch}(G_{cross}, \{1, 4\}) &= \text{PerfMatch}(G_{cross}, \{2, 3\}) = 0. \end{aligned}$$

These identities are illustrated in Fig. 3. In addition, $\text{PerfMatch}(G_{cross}, S) = 0$ whenever $|S|$ is odd. Thus the four boundary conditions for which the matching sum is non-zero represents the four possible configurations (empty/occupied) of a pair of crossing edges if they were attached to the vertices $\{1, 2, 3, 4\}$. For every edge crossing point of C_n one has to cut out a small disk centered at the crossing point and replace the interior of the disk by the gadget G_{cross} such that the four vertices $\{1, 2, 3, 4\}$ are attached to the four external edges, see Fig. 2. Let \tilde{C}_n be the resulting graph. By construction, \tilde{C}_n is planar. It remains to assign weights to edges of \tilde{C}_n such that

$$(29) \quad \text{PerfMatch}(\tilde{C}_n, \emptyset) = \text{Pf}(A).$$

Any edge of \tilde{C}_n falls into one of the four categories: (i) edge of C_n ; (ii) a section of some edge of C_n between two crossing gadgets; (iii) a section of some edge of C_n between a vertex of C_n and some crossing gadget; (iv) an edge that belongs to some crossing gadget. Note that the edges of type (iv) have been already assigned a weight, whereas any edge of type (i),(ii), and (iii) has a unique ancestor edge $e = (u, v)$ in C_n . Let us agree that for every edge $e = (u, v)$, $u < v$ of C_n we choose one of its descendants \tilde{e} in \tilde{C}_n and assign \tilde{e} the weight $A_{u,v}$, while all other

⁴One can gain some intuition about the extra sign factor in Eq. (27) if one thinks about the set of edges occupied by a perfect matching y as a family of "world lines" of fermionic particles. The contribution from y to $\text{Pf}(A)$ can be thought of as a quantum amplitude assigned to this family of world lines. Whenever two particles are exchanged the amplitude acquires an extra factor -1 .

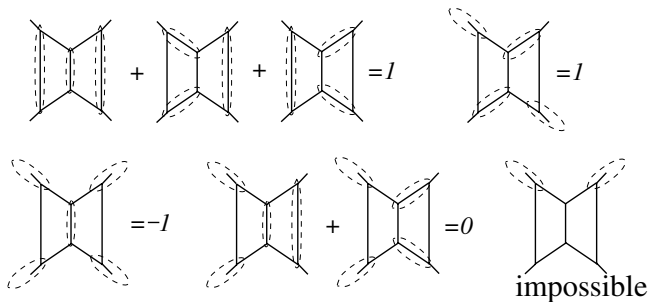


FIGURE 3. Matching sums of the graph G_{cross} corresponding to various boundary conditions.

descendants of e are assigned the weight 1. Since all descendants of e appear or do not appear in any perfect matching $M \in \mathcal{M}(\tilde{C}_n)$ simultaneously, we arrive to Eq. (29), that is, \tilde{C}_n is the desired graph G . It remains to count the number of vertices in \tilde{C}_n . There are $O(n^2)$ crossing gadgets each having $O(1)$ vertices. Thus \tilde{C}_n has $O(n^2)$ vertices. Since \tilde{C}_n is a planar graph it has $O(n^2)$ edges, see [24]. \square

Let \tilde{C}_n be a planar graph constructed above. Consider a subset of vertices $S \subseteq \{1, 2, \dots, n\}$ lying on the boundary of the disk. By repeating the arguments used in the proof of Lemma 3 one concludes that

$$(30) \quad \text{PerfMatch}(\tilde{C}_n, S) = \text{Pf}(A[S]) \quad \text{for all } S \subseteq \{1, 2, \dots, n\},$$

where $A[S]$ is a matrix obtained from A by removing all rows and columns $a \in S$. Theorem 3 follows from Eq. (30) and the following simple observation.

LEMMA 4. *Let T be a matchgate tensor of rank n with a parity $\epsilon(T)$ specified by its generating function*

$$(31) \quad T = C \exp\left(\frac{1}{2} \theta^T F \theta\right) \int D\mu \exp(\mu^T G \theta).$$

Then for all $x \in \{0, 1\}^n$

$$(32) \quad T(x) = C \epsilon(T) \text{Pf}\left(A(x 1^{k-n})\right), \quad \text{where } A = \begin{bmatrix} F & -G^T \\ G & 0 \end{bmatrix}.$$

The matrix A has size $k \times k$ with $n \leq k \leq 2n$.

Remark: As usual, $A(y)$ denotes a matrix obtained from A by removing all columns and rows a such that $y_a = 0$. We assume that $\epsilon(T) = 1$ ($\epsilon(T) = -1$) for even (odd) tensors.

PROOF. Theorem 2 asserts that T always has a generating function Eq. (31) where G has size $m \times n$ for some $m \leq n$. Thus $k = n + m \leq 2n$. Introducing a set of k Grassmann variables $\eta = (\theta_1, \dots, \theta_n, \mu_1, \dots, \mu_m)$ one can rewrite T as

$$T(\theta) = C \int D\mu \exp\left(\frac{1}{2} \eta^T A \eta\right).$$

Expanding the exponent one gets

$$\exp\left(\frac{1}{2}\eta^T A \eta\right) = \sum_{z \in \{0,1\}^k} \text{Pf}(A(z)) \eta(z).$$

Note that

$$\int D\mu \eta(z) = \begin{cases} (-1)^{m(z_1+\dots+z_n)} & \text{if } z_{n+1} = \dots = z_k = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Taking into account that m is even (odd) for even (odd) tensors and so is $z_1 + \dots + z_n$ we conclude that

$$(33) \quad T(\theta) = C\epsilon(T) \sum_{x \in \{0,1\}^n} \text{Pf}(A(x1^{k-n})) \theta(x),$$

that is $T(x) = C\epsilon(T) \text{Pf}(A(x1^{k-n}))$. \square

PROOF OF THEOREM 3. Let A be the $k \times k$ matrix constructed in Lemma 4 and \tilde{C}_k be the weighted planar graph constructed in Lemma 3 such that Eq. (30) holds for all $S \subseteq \{1, 2, \dots, k\}$. Therefore,

$$(34) \quad T(x) = C\epsilon(T) \text{PerfMatch}(\tilde{C}_k, \bar{x}0^{k-n}) \quad \text{for all } x \in \{0,1\}^n$$

where \bar{x} is obtained from x by flipping every bit. In order to transform Eq. (34) into Eq. (25) one can incorporate the factor $C\epsilon(T)$ into the matching sum by introducing an extra edge with a weight $C\epsilon(T)$ and adding one extra edge with weight 1 to every vertex $1, 2, \dots, n$ of the graph \tilde{C}_k in order to flip bits of x . \square

Although it is not necessary, let us mention that the reverse of Theorem 3 is also true, namely, a tensor T defined by Eq. (25) is always a matchgate. The easiest way to prove it is to represent the matching sum $\text{PerfMatch}(G, x)$ in Eq. (25) as a contraction of an open matchgate tensor network, see Section 4.3, in which every tensor has a linear generating function (thus simulating the perfect matching condition). Then one can use Corollary 4 to prove that T is a matchgate.

4. Contraction of matchgate tensor networks

4.1. Edge contractions. Consider a tensor network \mathcal{T} defined on a graph $G = (V, E)$ embedded to a surface Σ . Suppose one can find a region $D \subset \Sigma$ with topology of a disk such that D contains exactly two vertices $u, v \in V$ and several edges connecting u and v as shown on Fig. 4. We shall define a new tensor network \mathcal{T}' such that: (i) \mathcal{T}' coincides with \mathcal{T} outside D ; (ii) \mathcal{T}' contains only one vertex inside D ; (iii) contraction values of \mathcal{T} and \mathcal{T}' are the same. The operation of replacing \mathcal{T} by \mathcal{T}' will be referred to as an *edge contraction*. The new vertex obtained by contracting all edges connecting u and v inside D will be denoted $u \star v$.

Suppose there are b edges connecting u and v that lie inside the disk. Applying, if necessary, a cyclic shift of components to the tensors T_u and/or T_v we can assume that these edges correspond to the last b components of the tensor T_u and the first b components of T_v , see Fig. 4. Note that if the tensors under consideration are matchgates, the tensors obtained after the cyclic shift are also matchgates, see Corollary 2. In the new network \mathcal{T}' a pair of vertices u, v is replaced by a single vertex $u \star v$ with degree $d(u \star v) = d(u) + d(v) - 2b$. We define a new tensor $T_{u \star v}$ as

$$(35) \quad T_{u \star v}(x, y) = \sum_{z_1, \dots, z_b=0,1} T_u(x, z_b, z_{b-1}, \dots, z_1) T_v(z_1, \dots, z_{b-1}, z_b, y),$$

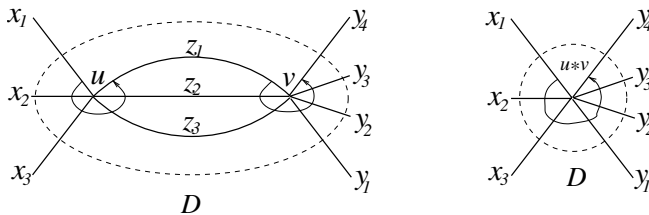


FIGURE 4. The ordering of edges before and after contraction of u and v .

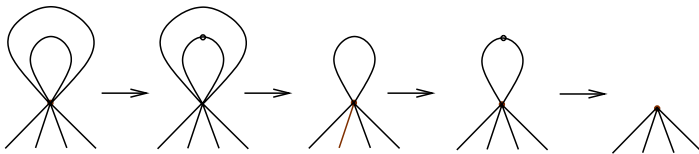


FIGURE 5. Contraction of self-loops can be reduced to edge contraction by adding dummy vertices.

where x and y can be arbitrary bit strings of length $d(u) - b$ and $d(v) - b$ respectively. By definition of the contraction value, $c(\mathcal{T}) = c(\mathcal{T}')$.

We shall also define a *self-loop contraction* as a special case of edge contraction. Namely, suppose one can find a region $D \subset \Sigma$ with topology of a disk such that D contains exactly one vertex $u \in V$ and several self-loops as shown on Fig. 5. We shall define a new tensor network \mathcal{T}' such that: (i) \mathcal{T}' coincides with \mathcal{T} outside D ; (ii) \mathcal{T}' contains one vertex without self-loops inside D ; (iii) contraction values of \mathcal{T} and \mathcal{T}' are the same. The operation of replacing \mathcal{T} by \mathcal{T}' will be referred to as a *self-loop contraction*. To define this operation, choose the most inner self-loop $\gamma \in E(u)$ introduce a dummy vertex v near the median of γ and assign a tensor $T_v(x_1, x_2) = \delta_{x_1, x_2}$ to this vertex. Clearly it does not change a contraction value of a network. Secondly, apply the edge contraction described above to the two edges connecting u and v . This reduces the number of self-loops by one. Repeat these two steps until all self-loops inside D are contracted.

It should be mentioned that self-loops $\gamma \in E(u)$ can be identified with elements of the fundamental group $[\gamma] \in \pi_1(\Sigma, u)$ of the surface Σ with a base point u . We do not allow to contract self-loops representing non-trivial homotopy classes (because it cannot be done efficiently for matchgate tensor networks).

4.2. Edge contraction as a convolution of generating functions. Let $\mathcal{T} = \{T_u\}_{u \in V}$ be a tensor network considered in the previous section. In order to describe each tensor T_u by a generating function $T_u(\theta)$ we shall introduce Grassmann variables $\theta_{u,1}, \dots, \theta_{u,d(u)}$ associated with the edges $e_1^u, \dots, e_{d(u)}^u \in E(u)$ incident to u such that

$$(36) \quad T_u(\theta) = \sum_{x \in \{0,1\}^n} T(x) (\theta_{u,1})^{x_1} (\theta_{u,2})^{x_2} \dots (\theta_{u,n})^{x_n}, \quad n \equiv d(u).$$

Similarly one can describe the contracted tensor $T_{u \star v}$ in Eq. (35) by a generating function

$$(37) \quad T_{u \star v}(\theta) = \sum_{x \in \{0,1\}^p} \sum_{y \in \{0,1\}^q} T_{u \star v}(x, y) (\theta_{u,1})^{x_1} \cdots (\theta_{u,p})^{x_p} (\theta_{v,b+1})^{y_1} \cdots (\theta_{v,b+q})^{y_q},$$

where $p \equiv d(u) - b$ and $q \equiv d(v) - b$. The goal of this section is to represent the function $T_{u \star v}(\theta)$ as an integral of $T_u(\theta)T_v(\theta)$ in which all variables associated with the edges to be contracted are integrated out.

Let $E(u, v)$ be a set of edges connecting u and v . For any edge $e \in E(u, v)$ such that e is labeled as $e_j^u \in E(u)$ and as $e_k^v \in E(v)$ denote

$$\theta(e) = \theta_{u,j} \theta_{v,k}, \quad \int D\theta(e) = \int d\theta_{v,k} \int d\theta_{u,j},$$

and

$$\int_{e \in E(u,v)} D\theta(e) = \prod_{e \in E(u,v)} \int D\theta(e).$$

Note that these definitions make sense only (u, v) is regarded as an ordered pair of vertices. Also note that the integrals $\int D\theta(e)$ over different edges commute, see Eq. (9), and thus one can take the integrals in an arbitrary order.

LEMMA 5. *Suppose the edges connecting u and v are ordered as shown on Fig. 4, i.e., these are the last b edges incident to u and the first b edges incident to v . Then*

$$(38) \quad T_{u \star v} = \int_{e \in E(u,v)} D\theta(e) T_u T_v \exp \left(\sum_{e \in E(u,v)} \theta(e) \right).$$

PROOF. By linearity it is enough to prove Eq. (38) for the case when T_u and T_v are monomials in the Grassmann variables, i.e.,

$$\begin{aligned} T_u &= (\theta_{u,1})^{x_1} \cdots (\theta_{u,p})^{x_p} (\theta_{u,p+1})^{z'_1} \cdots (\theta_{u,p+b})^{z'_b}, \\ T_v &= (\theta_{v,1})^{z_1} \cdots (\theta_{v,b})^{z_b} (\theta_{v,b+1})^{y_1} \cdots (\theta_{v,b+q})^{y_q}, \end{aligned}$$

where $p \equiv d(u) - b$ and $q \equiv d(v) - b$. By expanding the exponent one gets a sum of all possible monomials in which the two variables associated with any edge $e \in E(u, v)$ are either both present or both absent. Therefore the integral in Eq. (38) is zero unless $z_j = z'_{b+1-j}$ for all $j = 1, \dots, b$. Suppose this is the case. Then one gets after some rearrangement of variables

$$T_u T_v = (\theta_{u,1})^{x_1} \cdots (\theta_{u,p})^{x_p} \left(\prod_{e \in S(z)} \theta(e) \right) (\theta_{v,b+1})^{y_1} \cdots (\theta_{v,d(v)})^{y_q},$$

where $S(z) \subseteq E(u, v)$ denotes a set of edges e such that e is labeled as $e_k^v \in E(v)$ and $z_k = 1$. Substituting it into the integral Eq. (38), taking into account that $\theta(e)$ is a central element and that $\int D\theta(e) \theta(e) = 1$ one gets

$$T_{u \star v} = (\theta_{u,1})^{x_1} \cdots (\theta_{u,p})^{x_p} (\theta_{v,b+1})^{y_1} \cdots (\theta_{v,b+q})^{y_q}$$

which coincides with the desired expression Eq. (37). \square

COROLLARY 4. *Suppose T_u and T_v are matchgates. Then the contracted tensor $T_{u \star v}$ is also a matchgate.*

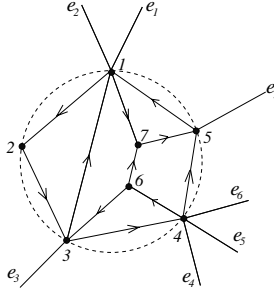


FIGURE 6. An open tensor network with 7 external edges equipped with a Kasteleyn orientation.

PROOF. Since cyclic shifts of indexes map matchgates to matchgates, see Corollary 2 in Section 3.2, we can assume that the edges of T_u and T_v are already ordered as required in Lemma 5. Represent T_u, T_v by their canonical generating functions, see Theorem 2. Using Eq. (38) one concludes that $T_{u \star v}(\theta)$ is a Gaussian integral $I(A, B)$ for some matrices A and B , see Eq. (11). Therefore, $T_{u \star v}$ is a matchgate, see Corollary 3 in Section 3.3. \square

Remark: Given the canonical generating functions for T_u and T_v , the canonical generating function for the contracted tensor $T_{u \star v}$ can be obtained straightforwardly using Eq. (38) and computing the resulting Gaussian integral $I(A, B)$ using Eq. (14). The details can be found in Appendix A.

4.3. Contraction of a planar subgraph in one shot. Suppose a planar connected graph $G = (V, E)$ is a part of a larger non-planar tensor network such that G is connected to the rest of the network by a subset of *external edges* $E_{ext} \subseteq E$. The remaining *internal edges* $E_{int} = E \setminus E_{ext}$ are the edges that can be contracted “locally” without touching the rest of the network. By abuse of definitions, we shall assume that the external edges have only one endpoint (the other endpoint belongs to the rest of the network) which belongs to the outer face of G , see Fig. 6. For convenience let us also assume that the graph G is embedded into a disk such that the external edges stick out from the disk as shown on Fig. 6. A network that consists of such a graph $G = (V, E)$ and a collection of tensors $\{T_u\}_{u \in V}$ will be referred to as an *open tensor network*. Throughout this section we shall consider only open tensor networks in which every tensor is a matchgate. Contraction of an open tensor network amounts to finding a tensor T_V of rank $|E_{ext}|$ obtained by contracting all internal edges of G . It follows from Corollary 4, Section 4.2 that T_V is a matchgate. The goal of the present section is to represent the generating function for the contracted tensor T_V as a convolution integral similar to Eq. (38) where the integration is taken over all internal edges.

An alternative strategy for computing T_V is to apply the edge contraction described in the previous section sequentially until all internal edges of G are contracted. Although it yields a polynomial-time algorithm this strategy is not very robust. An obvious drawback is that every edge contraction involves computing the Gaussian integral Eq. (14) which requires a matrix inversion. Contracting sequentially $O(n)$ edges would require $O(n)$ nested matrix inversions which may be

difficult or impossible to do if the matrix elements are specified with a finite precision. In order to reduce the number of nested matrix inversions one could organize the edge contractions into a sequence of rounds such that each round involves contractions of pairwise disjoint edges. The contractions involved in every round can be performed in parallel. The number of the rounds can be made $O(\log n)$ using the techniques developed by Fürer and Raghavachari [22]. We shall not pursue this strategy though because the approach described below allows one to compute T_V using only one matrix inversion.

The main result of this section is the following theorem.

THEOREM 4. *Consider an open matchgate tensor network on a planar graph $G = (V, E)$ with n vertices and m external edges. Assume that the tensors T_1, \dots, T_n are specified by their canonical generating function,*

$$T_j(\theta) = C_j \exp\left(\frac{1}{2} \theta^T A_j \theta\right) \int D\mu \exp(\mu^T B_j \theta).$$

Then the tensor T_V obtained by contracting all internal edges of G can be represented as a Gaussian integral

$$(39) \quad T_V(\eta) = \prod_{j=1}^n C_j \epsilon(T_j) \int D\theta \exp\left(\frac{1}{2} \theta^T A \theta + \theta^T B \eta\right).$$

Here A, B are matrices of size $k \times k$ and $k \times m$ for some $k = O((n+m)^2)$. Matrix elements of A and B are linear functionals of A_1, \dots, A_n and B_1, \dots, B_n . One can compute A and B in time $O(k)$. Furthermore, if G has bounded vertex degree then the same statement holds for $k = O(m+n)$.

Before going into technical details let us explain what is the main difficulty in representing the contracted tensor T_V by a single Gaussian integral. The point is that the convolution formula Eq. (38) holds only if the edges incident to the vertices u, v are ordered in a consistent way as shown on Fig. 4. If the orderings are not consistent, an extra sign may appear while commuting the variables living on the contracted edges towards each other. Assume one wants to contract the combined vertex $u \star v$ with some third vertex w . If the ordering of edges at the combined vertex $u \star v$ is not consistent with the ordering at w , one has to perform a cyclic shift of indexes in the tensor $T_{u \star v}$ and/or T_w before one can directly apply the formula Eq. (38) to $T_{u \star v}$ and T_w . Therefore, in general one can not represent the tensor $T_{u \star v \star w}$ obtained by contracting u, v, w as a single Gaussian integral.

In order to avoid the problem with inconsistent edge orderings we shall contract an open matchgate tensor network in two stages. At the first stage one simulates each tensor T_u by a matching sum of some planar graph as explained in Section 3.3. It yields an open tensor network in which every tensor has a linear generating function (since every vertex must have exactly one incident edge). At the second stage one represents the contraction of such a network by a single convolution integral analogous to Eq. (38). The problem with inconsistent edge ordering will be addressed by choosing a proper orientation on every edge (which affects the definition of monomials $\theta(e)$ in Eq. (38)). One can regard this approach as a generalization of the original Kasteleyn's method [8] to the case of a matching sum with "boundary conditions".

DEFINITION 3. *A tensor T is called linear if it has a linear generating function, $T = \sum_{a=1}^n w_a \theta_a$.*

Clearly, any linear tensor T can be mapped to $T(\theta) = \theta_1$ by a linear change of variables. Lemma 1 implies that $T(\theta) = \theta_1$ is a matchgate. Therefore any linear tensor is a matchgate, see Lemma 2.

DEFINITION 4. *Orientation of a graph $G = (V, E)$ is an antisymmetric matrix A of size $|V| \times |V|$ such that*

$$A_{u,v} = \begin{cases} \pm 1 & \text{if } (u,v) \in E, \\ 0 & \text{otherwise.} \end{cases}$$

An edge $(u,v) \in E$ is oriented from u to v iff $A_{u,v} = 1$.

Recall that we represent each tensor T_u by a generating function $T_u(\theta)$ that depends on Grassmann variables $(\theta_{u,1}, \dots, \theta_{u,d(u)})$ associated with the edges incident to u , see Eq. (36). Given an orientation A of the graph G and an edge $e = (u,v) \in E$ with the labels $e_j^u \in E(u)$ and $e_k^v \in E(v)$, define

$$(40) \quad \theta(e) = A_{u,v} \theta_{u,j} \theta_{v,k}, \quad \int D\theta(e) = A_{u,v} \int d\theta_{v,k} \int d\theta_{u,j},$$

and

$$\int_{e \in E_{int}} D\theta(e) = \prod_{e \in E_{int}} \int D\theta(e).$$

Note that $\theta(e)$ and $\int D\theta(e)$ are symmetric under the transposition of u and v .

LEMMA 6. *Let T_V be a tensor obtained by contraction of an open tensor network on a graph $G = (V, E)$. Assume that all tensors in the network are linear. Then there exists an orientation A and an ordering of the vertices $V = \{v_1, v_2, \dots, v_n\}$ such that*

$$(41) \quad T_V = \int_{e \in E_{int}} D\theta(e) T_{v_1} T_{v_2} \cdots T_{v_n} \exp \left(\sum_{e \in E_{int}} \theta(e) \right).$$

The orientation and the ordering can be found in time $O(n)$.

Remark 1: The generating function of T_V is defined for the ordering of the external edges in which they appear as one circumnavigates the boundary of the disk anticlockwise. The order of variables in T_V corresponds to the counterclockwise order of the external edges.

PROOF. Without loss of generality G is a 2-connected graph⁵. Then the boundary of the outer face of G is a closed loop without self-intersections. Let us denote it Γ_{out} . Mark some vertex in Γ_{out} that has at least one incident external edge (if there are no external edges, mark an arbitrary vertex). Let $\Gamma_{out} = \{1, 2, \dots, m\}$ be an ordered list of all vertices on the outer face of G corresponding to circumnavigating Γ_{out} anticlockwise starting from the marked vertex. Extend the ordering of vertices to the rest of V in an arbitrary way, so that $V = \{1, 2, \dots, n\}$ and the first m vertices belong to Γ_{out} .

⁵If G has a cut-vertex u one can always add an extra edge to some pair of nearest neighbors of u in order to make G 2-connected. The new edge must be assigned a zero weight in the two tensors it belongs to. Since the new edge does not contribute to T_V it can be safely removed at the end of the analysis.

DEFINITION 5. Let G be a planar graph with the vertices ordered as described above. A *Kasteleyn orientation (KO)* of G is an orientation A such that

- (1) The number of c.c.w. oriented edges in the boundary of any face of G is odd (except for the outer face).
- (2) $A_{1,2} = A_{2,3} = \dots = A_{m-1,m} = 1$.

Remark: The standard definition of a KO requires that (1) holds for all faces of G including the outer face and does not require (2), see for example [13]. By abuse of definitions we shall apply the term KO to orientations satisfying (1),(2). The standard definition is not suitable for our purposes because G may have odd number of vertices while the standard KO exists only on graphs with even number of vertices. The condition (2) is needed to ensure consistency between different "boundary conditions". Example of a KO is shown on Fig. 6.

PROPOSITION 3. Any planar graph has a KO. It can be found in a linear time.

We postpone the proof of the proposition until the end of the section. Let us choose the orientation A in Eq. (40) as a KO of the graph obtained from G by removing all external edges. Let us verify that the contracted tensor T_V can be written as in Eq. (41).

Indeed, let $S \subseteq E_{ext}$ be a subset of external edges such that any vertex in $\{1, \dots, m\}$ has at most one incident edge from S . (Below we shall consider only such sets S without explicitly mentioning it.) Let ∂S be a set of vertices that have an incident edge from S (clearly all such vertices belong to the outer face). For any S as above and any ∂S -imperfect matching $M \in \mathcal{M}(G, \partial S)$ define a subset of Grassmann variables

$$\Omega(S, M) = \{(u, j) : u \in V, \text{ and } e_j^u \in S \cup M\}.$$

In other words, $(u, j) \in \Omega(S, M)$ iff $\theta_{u,j}$ is a Grassmann variable that live on some edge of $S \cup M$. Note that there are two Grassmann variables living on any internal edge and one variable living on any external edge. Thus for any S and M the set $\Omega(S, M)$ contains n variables. Define a normally ordered monomial

$$(42) \quad \prod_{(u,j) \in \Omega(S,M)} \theta_{u,j}$$

as a product of all variables in $\Omega(S, M)$ ordered according to

$$(43) \quad (\theta_{1,1}, \dots, \theta_{1,d(1)}, \theta_{2,1}, \dots, \theta_{2,d(2)}, \dots, \theta_{n,1}, \dots, \theta_{n,d(n)}).$$

Define also M -ordered monomial

$$(44) \quad \prod_{(u,j) : e_j^u \in S} \theta_{u,j} \prod_{e \in M} \theta(e),$$

where the order in the first product must agree with the chosen ordering of edges in E_{ext} , see Fig. 6. Clearly the two products Eqs. (42,44) coincide up to a sign that we shall denote $\text{sgn}(M)$. In order to prove Lemma 6 it suffices to show that

$$(45) \quad \text{sgn}(M) = 1 \quad \text{for all } \partial S\text{-imperfect matchings } M, \text{ for all } S \subseteq E_{ext}.$$

Indeed, denoting $T_u = \sum_{j=1}^{d(u)} w_j^u \theta_{u,j}$ one can rewrite Eq. (41) as

$$\begin{aligned}
 T_V &= \sum_{S \subseteq E_{ext}} \sum_{M \in \mathcal{M}(G, \partial S)} \int_{e \in E_{int}} D\theta(e) \prod_{(u,j) \in \Omega(S,M)} w_j^u \theta_{u,j} \prod_{e \notin M} \theta(e) \\
 (46) \quad &= \sum_{S \subseteq E_{ext}} \prod_{(u,j): e_j^u \in S} \theta_{u,j} \sum_{M \in \mathcal{M}(G, \partial S)} \text{sgn}(M) \prod_{(u,j): e_j^u \in M} w_j^u.
 \end{aligned}$$

Assuming $\text{sgn}(M) \equiv 1$ one can identify the sum over $M \in \mathcal{M}(G, \partial S)$ with the component of the contracted tensor T_V in which the subset S of external edges carries index 1.

Note that for any $S \subseteq E_{ext}$ and any ∂S -imperfect matching M each vertex $u \in V$ contributes exactly one variable to $\Omega(S, M)$. Indeed, at every vertex $u \in V$ there is either one incident edge from M or one incident external edge. All other edges incident to u and the variables living on these edges can be ignored as far as computation of $\text{sgn}(M)$ is concerned. Therefore one can compute the sign $\text{sgn}(M)$ by introducing auxiliary Grassmann variables $\eta = (\eta_1, \dots, \eta_n)$ associated with vertices of G and comparing the normal ordering of η (the one in which the indexes increase from the left to the right) with the M -ordering of η , namely

$$\prod_{u \in \partial S} \eta_u \prod_{e \in M} \eta(e) = \text{sgn}(M) \eta_1 \eta_2 \cdots \eta_n, \quad \text{where} \quad \eta(e) = A_{u,v} \eta_u \eta_v \quad \text{if} \quad e = (u, v).$$

Here the ordering in the first product is normal while the ordering in the second product may be arbitrary since $\eta(e)$ is a central element. Consider any subsets $S, S' \subseteq E_{ext}$. Given any ∂S -imperfect matching M and $\partial S'$ -imperfect matching M' define a relative sign

$$(47) \quad \text{sgn}(M, M') \stackrel{\text{def}}{=} \text{sgn}(M) \text{sgn}(M'),$$

such that

$$(48) \quad \prod_{u \in \partial S} \eta_u \prod_{e \in M} \eta(e) = \text{sgn}(M, M') \prod_{u \in \partial S'} \eta_u \prod_{e \in M'} \eta(e).$$

In order to compute $\text{sgn}(M, M')$ consider the symmetric difference $M \oplus M'$. It consists of a disjoint union of even-length cycles C_1, \dots, C_p and open paths $\Gamma_1, \dots, \Gamma_q$ such that every path Γ_j has both its endpoints in the symmetric difference $\partial S \oplus \partial S'$. Given a path Γ_j with endpoints $s, t \in \partial S \oplus \partial S'$, $s < t$ let us orient Γ_j from s to t . Now one can compute the relative sign as follows.

PROPOSITION 4. *Consider any subsets $S, S' \subseteq E_{ext}$. Let C_1, \dots, C_p and $\Gamma_1, \dots, \Gamma_q$ be the cycles and the paths formed by $M \oplus M'$ for some ∂S -imperfect matching M and some $\partial S'$ -imperfect matching M' . For a path Γ_j connecting vertices $s, t \in \partial S \oplus \partial S'$ on the outer face such that $s < t$ let $\omega(\Gamma_j) = 1$ if the interval (s, t) contains odd number of vertices from ∂S and $\omega(\Gamma_j) = 0$ if this number is even. Then*

$$(49) \quad \text{sgn}(M, M') = (-1)^p \prod_{j=1}^p \Phi(C_j) \prod_{k=1}^q (-1)^{\omega(\Gamma_k)} \Phi(\Gamma_k),$$

where

$$\Phi(C_j) = \prod_{(u,v) \in C_j} A_{u,v} \quad \text{and} \quad \Phi(\Gamma_k) = \prod_{(u,v) \in \Gamma_k} A_{u,v}.$$

Remark 1: The definition of $\omega(\Gamma_j)$ is symmetric under exchange of S and S' . Indeed, the overall number of vertices from $\partial S \oplus \partial S'$ contained in the interval (s, t) is even since these vertices are pairwise connected by Γ 's. The remaining vertices of (s, t) either belong to both sets S, S' or belong to neither of them.

Remark 2: The product $\prod_{(u,v) \in \Gamma_k} A_{u,v}$ gives the parity of the number of edges in Γ_k whose orientation determined by A disagrees with the chosen orientation of Γ_k . The product $\Phi(C_j)$ does not depend on how one chooses orientation of C_j since every cycle C_j has even length.

PROOF. Indeed, one can easily check that for every cycle C_j one has

$$(50) \quad \prod_{e \in C_j \cap M} \eta(e) = -\Phi(C_j) \prod_{e \in C_j \cap M'} \eta(e).$$

Therefore changing the M -ordering to the M' -ordering in a cycle C_j contributes a factor $-\Phi(C_j)$ to the relative sign $\text{sgn}(M, M')$. Consider now a path Γ_j connecting vertices $s, t \in \partial S \oplus \partial S'$ where $s < t$. Let us argue that changing the M -ordering to the M' -ordering on the path Γ_j contributes a factor $(-1)^{\omega(\Gamma_j)} \Phi(\Gamma_j)$ to the relative sign $\text{sgn}(M, M')$. Indeed, one can easily check the following identities:

$$\begin{aligned} s, t \in S & : \quad \eta_s \eta_t \prod_{e \in \Gamma_j \cap M} \eta(e) = \Phi(\Gamma_j) \prod_{e \in \Gamma_j \cap M'} \eta(e), \\ s, t \in S' & : \quad \text{the same as above up to } M \leftrightarrow M', \\ s \in S, t \in S' & : \quad \eta_s \prod_{e \in \Gamma_j \cap M} \eta(e) = \Phi(\Gamma_j) \eta_t \prod_{e \in \Gamma_j \cap M'} \eta(e), \\ s \in S', t \in S & : \quad \text{the same as above up to } M \leftrightarrow M'. \end{aligned}$$

Consider as example the case $s, t \in S$. Bringing the variables η_s and η_t together in the monomial $\prod_{u \in \partial S} \eta_u$ introduces an extra sign $(-1)^{\omega(\Gamma_j)}$. Taking into account that $\eta(e)$ are central elements and using the first identity above one concludes that

$$\prod_{u \in \partial S} \eta_u \prod_{e \in \Gamma_j \cap M} \eta(e) = (-1)^{\omega(\Gamma_j)} \Phi(\Gamma_j) \prod_{u \in \partial S \setminus \{s, t\}} \eta_u \prod_{e \in \Gamma_j \cap M'} \eta(e).$$

Other three cases can be considered analogously using Remark 1 above. Combining it with Eq. (50) one arrives to Eq. (49). \square

Let us proceed with the proof of Lemma 6. The first condition in the definition of KO implies⁶ that $\Phi(C_j) = -1$ for all cycles C_j . Indeed, consider any particular cycle C_j and let N_0, N_1, N_2 be the number of vertices, edges, and faces in the subgraph bounded by C_j . The Euler formula implies that $N_0 + N_2 - N_1 = 1$. Denote also N_1^{int} the number of *internal* edges, i.e., edges having at least one endpoint in the interior of C_j . Since C_j has even length, N_1^{int} has the same parity as N_1 . Furthermore, since all vertices of the subgraph bounded by C_j are paired by M (and by M'), N_0 is even. Since $\Phi(C_j)$ can be regarded as a parity of c.c.w. oriented edges in C_j and each internal edge is c.c.w. oriented with respect to one of the adjacent faces the property (1) of KO yields

$$(51) \quad \Phi(C_j) = (-1)^{N_2 + N_1^{int}} = (-1)^{N_2 + N_1} = (-1)^{1 + N_0} = -1.$$

⁶This is the well-known property of a Kasteleyn orientation which we prove below for the sake of completeness.

Therefore Proposition 4 implies

$$(52) \quad \text{sgn}(M, M') = \prod_{k=1}^q (-1)^{\omega(\Gamma_k)} \Phi(\Gamma_k).$$

Let us now show that

$$(53) \quad (-1)^{\omega(\Gamma_k)} \Phi(\Gamma_k) = 1$$

for all paths Γ_k . Indeed, let $s, t \in S \oplus S'$ be the starting and the ending vertices of Γ_k . Consider a path Γ_k^* obtained by passing from t to s along the boundary of the outer face Γ_{out} in the clockwise direction. Let N_0, N_1, N_2 be the number of vertices, edges, and faces in the subgraph bounded by a cycle $\Gamma_k \cup \Gamma_k^*$. Denote also N_1^{int} the number of edges that have at least one endpoint in the interior of $\Gamma_k \cup \Gamma_k^*$. The Euler formula implies that $N_0 + N_2 - N_1 = 1$. Note that $\Phi(\Gamma_k)$ can be regarded as the parity of the number of edges in Γ_k whose orientation determined by A corresponds to c.c.w. orientation of the cycle $\Gamma_k \cup \Gamma_k^*$. Repeating the arguments leading to Eq. (51) and noting that all edges of the cycle $\Gamma_k \cup \Gamma_k^*$ belonging to Γ_k^* are oriented c.c.w. one gets

$$(54) \quad \Phi(\Gamma_k) = (-1)^{|\Gamma_k^*| + N_2 + N_1^{int}} = (-1)^{|\Gamma_k| + N_2 + N_1} = (-1)^{|\Gamma_k| + N_0 + 1}.$$

Here $|\Gamma_k|$ and $|\Gamma_k^*|$ are the numbers of edges in the two paths. Consider three possibility:

Case 1: $s, t \in \partial S$. Then $|\Gamma_k|$ is odd and thus $\Phi(\Gamma_k) = (-1)^{N_0}$. All N_0 vertices of the graph bounded by $\Gamma_k \cup \Gamma_k^*$ are paired by the matching M except for s, t and those belonging to ∂S and lying on the interval (s, t) . Therefore the parity of N_0 coincides with $\omega(\Gamma_k)$ and we arrive to Eq. (53).

Case 2: $s, t \in \partial S'$. The same as Case 1 (see Remark 1 after Proposition 4).

Case 3: $s \in \partial S, t \in \partial S'$ (or vice versa). Then $|\Gamma_k|$ is even and thus $\Phi(\Gamma_k) = (-1)^{N_0+1}$. All N_0 vertices of the graph bounded by $\Gamma_k \cup \Gamma_k^*$ are paired by the matching M except for s (or except for t) and those belonging to ∂S and lying on the interval (s, t) . Therefore the parity of N_0 coincides with $\omega(\Gamma_k) + 1$ and we arrive to Eq. (53).

Combining Eqs. (51,53) and Proposition 4 we conclude that $\text{sgn}(M, M') = 1$ for all M and M' . Thus either $\text{sgn}(M) = 1$ for all M or $\text{sgn}(M) = -1$ for all M . One can always exclude the latter possibility by applying a *gauge transformation* to the orientation A . A gauge transformation at a vertex $u \in V$ reverses orientation of all edges incident to u . Let us say that a vertex $u \in V$ is *internal* if does not belong to the outer face of G . Clearly a gauge transformation at any internal vertex u maps a KO to a KO and flips the sign $\text{sgn}(M)$ for all M . Thus it suffices to consider the case when G does not have internal vertices (i.e. G is an outerplanar graph). If $m = n$ is even, a matching $M = \{(1, 2), (3, 4), \dots, (m-1, m)\}$ has sign $\text{sgn}(M) = 1$ due to property (1) of a KO and thus all matchings have sign $+1$. If $m = n$ is odd one can apply the same argument using a matching $M = \{(2, 3), (4, 5), \dots, (m-1, m)\}$ (recall that the vertex 1 has at least one external edge and thus it can be omitted in M). \square

PROOF OF THEOREM 4. Let n_e be the number of internal edges in the graph G , so that $|E| = m + n_e$. Since G is a planar graph, $n_e = O(n)$, see for example [24], and thus $|E| = O(n + m)$. Denote degree of a vertex $u \in V$ by $d(u)$ (it includes both internal and external edges). Applying Theorem 3 one can simulate the tensor

T_u at any vertex $u \in V$ by a matching sum of some planar graph G_u with $O(d(u)^2)$ vertices. Combining the graphs G_u together one gets an open tensor network $G' = (V', E')$ in which all tensors are linear. The network G' has m external edges. The number of vertices n' in the network G' can be bounded as $n' = \sum_{u \in V} O(d(u)^2) = O((\sum_{u \in V} d(u))^2) = O(|E|^2) = O((m+n)^2)$. If G has bounded degree one gets $n' = \sum_{u \in V} O(d(u)^2) = O(n)$. Thus in both cases $n' = O(k)$, where k is defined in the statement of the theorem. It follows from Theorem 3 that the edge weights in the matching sums are linear functions of the matrix elements of A_1, \dots, A_n and B_1, \dots, B_n . Let n'_e be the number of internal edges in G' . Since G' is a planar graph, $n'_e = O(n') = O(k)$. Thus the total number of edges in G' is $|E'| = n'_e + m = O(k)$. Invoking Lemma 6 we need to introduce a pair of Grassmann variables for every internal edge of G' and one variable for every external edge. Thus the total number of Grassmann variables is $O(k)$. It determines the number of variables in the vector θ in Eq. (39). Representing linear tensors T_j as Gaussian integrals, namely

$$T_j = \int d\mu \exp(\mu T_j),$$

one can combine the multiple integrals in Eq. (41) into a single Gaussian integral Eq. (39) with the matrix A having a dimension $O(k) \times O(k)$ and B having a dimension $O(k) \times m$. Thus A and B have the desired properties. \square

PROOF OF PROPOSITION 3. Let $G = (V, E)$ be a planar graph with n vertices such that the outer face of G is a simple loop. An orientation A satisfying (1) can be constructed using the algorithm of [13]. For the sake of completeness we outline it below. Let $G^* = (V^*, E)$ be the dual graph such that each face of G contributes one vertex to G^* (including the outer face). Let T be a spanning tree of G^* such that the root of T is the outer face of G . One can find T in time $O(|V| + |E|) = O(n)$ since for planar graphs $|E| = O(|V|)$. Assign an arbitrary orientation to those edges of G that do not belong to T . By moving from the leaves of T to the root assign the orientation to all edges of T . Note that for every vertex u of T which is not the root the orientation of an edge e connecting u to its ancestor is uniquely determined by (1). We obtained an orientation of all edges of G satisfying (1).

In order to satisfy (2) one can apply a series of *gauge transformations*. A gauge transformation at a vertex $u \in V$ reverses orientation of all edges incident to u . Clearly it preserves the property (1). Applying if necessary a gauge transformation at the vertices $\{1, 2, \dots, m-1\}$ one can satisfy (2). \square

4.4. Contraction of matchgate networks with a single vertex. In this section we explain how to contract a matchgate tensor network \mathcal{T} that consists of a single vertex u with m self-loops embedded into a surface Σ of genus g without self-intersections. Example of such a network with $m = 3$ and $g = 1$ is shown on Fig. 7. Let T be a tensor of rank $2m$ associated with u . Clearly the contraction value $c(\mathcal{T})$ depends only on the pairing pattern indicating what indexes of T are contracted with each other. It will be convenient to represent the pairing pattern by a *pairing graph* $P = (V, E)$ with a set of vertices $V = \{1, 2, \dots, 2m\}$ such that a pair of vertices (a, b) is connected by an edge iff the indexes a, b of the tensor T are contracted with each other (connected by a self-loop). By definition P consists of m disjoint edges. Let us embed P into a disk such that all the vertices of P lie on the boundary of the disk and their order corresponds to circumnavigating the boundary anticlockwise. The edges of P are represented by arcs lying inside the

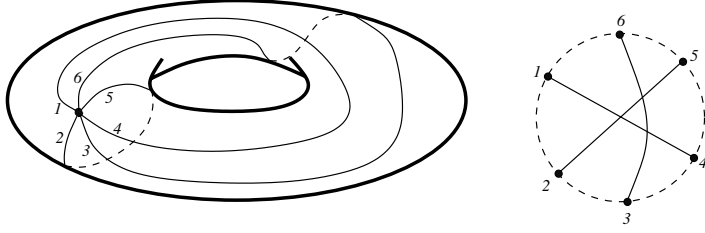


FIGURE 7. Left: a tensor network with a single vertex embedded into a torus. Right: the pairing graph P .

disk, see Fig. 7. One can always draw the arcs such that there are only pairwise intersection points.

Introduce an auxiliary tensor R of rank $2m$ such that

$$R(x) = \begin{cases} 1 & \text{if } x_a = x_b \text{ for all } (a, b) \in E, \\ 0 & \text{if } x_a \neq x_b \text{ for some } (a, b) \in E. \end{cases}$$

The contraction value of \mathcal{T} can be represented as

$$(55) \quad c(\mathcal{T}) = \sum_{x \in \{0,1\}^{2m}} T(x) R(x).$$

Let $\theta = (\theta_1, \dots, \theta_{2m})$ and $\eta = (\eta_1, \dots, \eta_{2m})$ be Grassmann variables and $T(\theta)$, $R(\eta)$ be the generating functions of T and R .

PROPOSITION 5. *Let $\epsilon(T) = 0, 1$ for even and odd tensors T respectively. Then*

$$(56) \quad c(\mathcal{T}) = i^{\epsilon(T)} \int D\theta \int D\eta T(\theta) R(\eta) \exp(i\theta^T \eta).$$

PROOF. A non-zero contribution to the integral comes from the terms in which $T(\theta)$ contributes monomial $T(x)\theta(x)$ and $R(\eta)$ contributes monomial $R(x)\eta(x)$ for some $x \in \{0,1\}^{2m}$. A simple algebra shows that for any $x \in \{0,1\}^{2m}$ one has the following identity

$$\theta(x)\eta(x) \prod_{a: x_a=0} i\theta_a\eta_a = i^{-|x|} (-1)^{|x|(|x|-1)/2} \theta(1^{2m})\eta(1^{2m}),$$

where $|x|$ is the Hamming weight of x . Taking into account that $T(x) = 0$ unless $|x|$ has parity $\epsilon(T)$ one gets

$$i^{-|x|} (-1)^{|x|(|x|-1)/2} = i^{-\epsilon(T)}.$$

Since $\int D\theta \int D\eta \theta(1^{2m})\eta(1^{2m}) = 1$, one gets Eq. (56). \square

In general R is not a matchgate tensor because the chosen planar embedding of the pairing graph may have edge crossing points. For example, assume that P has 4 vertices $\{1, 2, 3, 4\}$ and two edges $(1, 3)$, $(2, 4)$ (which can be realized on a torus). Then the non-zero components of R are $R(0000) = R(1010) = R(0101) = R(1111) = 1$. Substituting them into the matchgate identities Eq. (2) for even rank-4 tensors one concludes that R is not a matchgate.

Let us order the edges of P in an arbitrary way, say, $E = \{e_1, e_2, \dots, e_m\}$. For any edges $e_p, e_q \in E$ let $N_{p,q}$ be the the number of self-intersections of e_p, e_q in the planar embedding shown on Fig. 7. Since we assumed that all intersections are pairwise, $N_{p,q}$ takes only values 0, 1, i.e., N is a symmetric binary matrix. Let us

also agree that $N_{p,p} = 0$. We shall see later that the tensor R can be represented as a linear combination of 2^r matchgate tensors, where r is a binary rank of the matrix N . It is crucial that the rank of N can be bounded by the genus g of the surface Σ .

LEMMA 7. *The matrix N has binary rank at most $2g$.*

PROOF. Let us cut a small disk D centered at the vertex u from the surface Σ , embed the pairing graph P into the disk D as shown on Fig. 7 and glue the disk back to the surface Σ . Thus given any self-loop α connecting indexes a and b of the tensor T , a small section of α lying inside D is replaced by an edge $e = (a, b) \in E$ of the pairing graph. We get a family of m closed loops embedded into Σ . The loops may have pairwise intersection points inside the disk D . Let α_p be a loop that contains an edge $e_p \in E$. To every loop α_p one can assign its homological class $[\alpha_p] \in H_1(\Sigma, \mathbb{Z}_2)$ in the first homological group of Σ with binary coefficients. Since all intersection points between the loops are contained in the disk D , we get

$$N_{p,q} = \omega([\alpha_p], [\alpha_q]),$$

where $\omega : H_1(\Sigma, \mathbb{Z}_2) \times H_1(\Sigma, \mathbb{Z}_2) \rightarrow \{0, 1\}$ is the intersection form. It is well known that the intersection form defined on a surface Σ of genus g has rank $2g$. Therefore, N has rank at most $2g$. \square

Given any edge $e \in E$, let $l(e), r(e) \in V$ be the two endpoints of e such that $l(e) < r(e)$. Denote $\eta(e) = \eta_{l(e)} \eta_{r(e)}$. The generating function for the tensor R can be written as

$$(57) \quad R(\eta) = \sum_{y \in \{0,1\}^m} (-1)^{\frac{1}{2} y^T N y} \prod_{e \in y} \eta(e), \quad \text{where } \eta(e) = \eta_{l(e)} \eta_{r(e)}.$$

Here we identified a binary string $y \in \{0, 1\}^m$ with the subset of edges $e_a \in E$ such that $y_a = 1$. Indeed, for any $x \in \{0, 1\}^{2m}$ such that $R(x) = 1$ one has to regroup the factors in $\eta(x)$ to bring together variables corresponding to the same edge. It yields an extra minus sign for every pair of intersecting edges in y . Since every pair of edges e_a, e_b contributes a sign $(-1)^{N_{a,b} y_a y_b}$, we arrive to Eq. (57).

Consider binary Fourier transform of the function $(-1)^{\frac{1}{2} y^T N y}$,

$$(58) \quad f(z) \stackrel{\text{def}}{=} \frac{1}{2^m} \sum_{y \in \{0,1\}^m} (-1)^{\frac{1}{2} y^T N y + z \cdot y}, \quad z \in \{0, 1\}^m.$$

Clearly $f(z) = 0$ unless $z \in \text{Ker}(N)^\perp$, where $\text{Ker}(N) = \{y \in \{0, 1\}^m : Ny = 0\}$ is the zero subspace of N . If N has rank r , the zero subspace of N has dimension $m - r$ and thus $\text{Ker}(N)^\perp$ has dimension r . Let us order all the vectors of $\text{Ker}(N)^\perp$ in an arbitrary way

$$\text{Ker}(N)^\perp = \{z^1, \dots, z^{2^r}\}.$$

Applying the reverse Fourier transform one gets

$$(59) \quad (-1)^{\frac{1}{2} y^T N y} = \sum_{a=1}^{2^r} f(z^a) (-1)^{y \cdot z^a}.$$

By Lemma 7 the number of terms in the sum above is bounded by 2^{2g} . Substituting Eq. (59) into Eq. (57) we arrive to

$$(60) \quad R(\eta) = \sum_{a=1}^{2^r} f(z^a) \exp \left(\sum_{e \in E} (-1)^{(z^a)_e} \eta(e) \right),$$

where $(z^a)_e$ is the component of the vector z^a corresponding to an edge e . It shows that R is indeed a linear combination of 2^r matchgate tensors with $r \leq 2g$.

In order to get an explicit formula for the contraction value Eq. (55) let us introduce an auxiliary $2m \times 2m$ matrix

$$A_{j,k} = \begin{cases} +1 & \text{if } j = l(e), k = r(e) \text{ for some } e \in E, \\ -1 & \text{if } j = r(e), k = l(e) \text{ for some } e \in E \\ 0 & \text{otherwise} \end{cases}$$

Introduce also auxiliary diagonal $2m \times 2m$ matrices D^a , $a = 1, \dots, 2^r$ such that

$$(D^a)_{j,j} = \begin{cases} (-1)^{(z^a)_e} & \text{if } j = l(e) \text{ for some } e \in E, \\ 1 & \text{otherwise.} \end{cases}$$

Then Eq. (60) can be rewritten as

$$(61) \quad R(\eta) = \sum_{a=1}^{2^r} f(z^a) \exp \left(\frac{1}{2} \eta^T D^a A D^a \eta \right).$$

Theorem 2 implies that T can be described by a generating function

$$T(\theta) = C \exp \left(\frac{1}{2} \theta^T F \theta \right) \int D\mu \exp (\mu^T G \theta),$$

where F and G have size $2m \times 2m$ and $k \times 2m$ for some even integer $0 \leq k \leq 2m$. Using Eq. (56) one can express the contraction value $c(T)$ as a linear combination of 2^r Gaussian integrals

$$(62) \quad c(T) = C \sum_{a=1}^{2^r} f(z^a) \int D\theta D\eta D\mu \exp \left(\frac{1}{2} \theta^T F \theta + \frac{1}{2} \eta^T D^a A D^a \eta + \mu^T G \theta + i \theta^T \eta \right).$$

Introducing a $(4m + k) \times (4m + k)$ matrix

$$M^a = \begin{bmatrix} F & iI & -G^T \\ -iI & -D^a A D^a & 0 \\ G & 0 & 0 \end{bmatrix}$$

one finally gets

$$(63) \quad c(T) = C \sum_{a=1}^{2^r} f(z^a) \text{Pf} (M^a).$$

Computing $\text{Pf} (M^a)$ requires time $O(m^3)$. Lemma 7 implies that the number of terms in the sum is at most 2^{2g} . Finally, as we show below one can compute $f(z^a)$ in time $O(m^3)$. Thus $c(T)$ can be computed in time $O(m^3) 2^{2g}$.

PROPOSITION 6. *The function $f(z)$ in Eq. (58) can be represented as*

$$(64) \quad f(z) = \frac{1}{2^{r/2}} (-1)^{\frac{1}{2} z^T M z}$$

for some matrix M computable in time $O(m^3)$.

PROOF. Using Gaussian elimination any symmetric binary matrix N with zero diagonal can be represented as $N = U^T \tilde{N} U$, where U is a binary invertible matrix and \tilde{N} is a block diagonal matrix with 2×2 blocks,

$$\tilde{N} = \bigoplus_{j=1}^{r/2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In particular, the rank of N is always even. The matrix U can be found in time $O(m^3)$. Performing a change of variable $y \rightarrow Uy$ in Eq. (58) one gets

$$(65) \quad f(z) = \frac{1}{2^m} \sum_{y \in \{0,1\}^m} (-1)^{\sum_{j=1}^{r/2} y_{2j-1} y_{2j} + \tilde{z} \cdot y}, \quad \tilde{z} = (U^{-1})^T z.$$

It follows that $f(z) = 0$ unless $\tilde{z}_{r+1} = \dots = \tilde{z}_m = 0$. Using an identity

$$(-1)^{x_1 \cdot x_2} = \frac{1}{2} \sum_{y_1, y_2=0,1} (-1)^{y_1 \cdot y_2 + y_1 \cdot x_1 + y_2 \cdot x_2}$$

one can rewrite Eq. (65) as

$$f(z) = \frac{1}{2^{r/2}} (-1)^{\sum_{j=1}^{r/2} \tilde{z}_{2j-1} \tilde{z}_{2j}} = \frac{1}{2^{r/2}} (-1)^{\frac{1}{2} z^T U^{-1} \tilde{N} (U^{-1})^T z}.$$

We get the desired expression Eq. (64) with $M = U^{-1} \tilde{N} (U^{-1})^T$. \square

4.5. The main theorem. Theorem 1 can be obtained straightforwardly from Theorem 4 and the contraction algorithm for a network with a single vertex, see Section 4.4. Indeed, let M be a planar cut of G with m edges and G_M be a subgraph obtained from G by removing all edges of M . By definition G_M is contained in some region D with topology of a disk. Without loss of generality D contains no edges from M (otherwise one can remove these edges from M getting a planar cut with a smaller number of edges). Thus one can regard G_M as an open tensor network with $2m$ external edges. Since G_M contains all vertices of G , the network obtained by contraction of G_M consists of a single vertex and m self-loops. As explained in the previous section, one can compute the contraction value of such a network in time $O(m^3) 2^{2g}$.

In order to contract G_M one has to compute the Gaussian integral Eq. (39). Theorem 4 guarantees that this integral involves matrices of size k , where $k = O((n+m)^2)$ or $k = O(n+m)$ depending on whether the graph G has bounded vertex degree. As explained in Section 2.4 the Gaussian integral with matrices of size k can be computed in time $O(k^3)$. Combining the two parts together one gets Theorem 1.

Acknowledgements

The author acknowledge support by DTO through ARO contract number W911NF-04-C-0098.

Appendix A

Suppose T_u and T_v are matchgate tensors specified by their canonical generating functions as in Eq. (17), that is

$$T_\alpha = C_\alpha \exp\left(\frac{1}{2} \theta_\alpha^T A_\alpha \theta_\alpha\right) \int D\mu_\alpha \exp(\mu_\alpha^T B_\alpha \theta_\alpha), \quad \text{where } \alpha = u, v.$$

Here $\theta_u = (\theta_{u,1}, \dots, \theta_{u,d(u)})$ and $\theta_v = (\theta_{v,1}, \dots, \theta_{v,d(v)})$ are the two sets of Grassmann variables associated with the vertices u and v . Denote also $\epsilon(T)$ the parity of a matchgate tensor T , that is, $\epsilon(T) = 0$ ($\epsilon(T) = 1$) for even (odd) tensor T . In the remainder of this section we explain how to express the canonical generating function for the contracted tensor $T_{u \star v}$, see Eqs. (37,38), in terms of the matrices A_α, B_α .

Applying Eq. (38) one gets

$$(66) \quad T_{u \star v} = C_u C_v \int_{e \in E(u,v)} D\theta(e) \int D\mu_u \int D\mu_v \exp[f(\theta_u, \theta_v, \mu_u, \mu_v)],$$

where

$$f(\theta_u, \theta_v, \mu_u, \mu_v) = \sum_{\alpha=u,v} \frac{1}{2} \theta_\alpha^T A_\alpha \theta_\alpha + \mu_\alpha^T B_\alpha \theta_\alpha + \sum_{e \in E(u,v)} \theta(e).$$

Let us split the vectors of Grassmann variables θ_u, θ_v into external and internal parts,

$$\theta_u = (\theta_u^e, \theta_u^i) \quad \text{and} \quad \theta_v = (\theta_v^i, \theta_v^e),$$

such that all internal variables are integrated out in $T_{u \star v}$. Then one can rewrite the expression Eq. (66) as a product of a Gaussian exponent and the standard Gaussian integral $I(K, L)$, see Eqs. (13,14), for some matrices K, L defined below,

$$(67) \quad T_{u \star v}(\tau) = C_u C_v (-1)^{\frac{b(b-1)}{2} + \epsilon(T_u)\epsilon(T_v)} \exp\left(\frac{1}{2} \tau^T H \tau\right) \int D\eta \exp\left(\frac{1}{2} \eta^T K \eta + \eta^T L \tau\right).$$

Here we introduced auxiliary vectors of Grassmann variables $\tau = (\theta_u^e, \theta_v^e)$, $\eta = (\theta_u^i, \theta_v^i, \mu_u, \mu_v)$. The matrices H, K, L above will be defined using a partition of matrices A_α, B_α into "internal" and "external" blocks as follows:

$$A_u = \begin{bmatrix} A_u^{ee} & A_u^{ei} \\ A_u^{ie} & A_u^{ii} \end{bmatrix}, \quad A_v = \begin{bmatrix} A_v^{ii} & A_v^{ie} \\ A_v^{ei} & A_v^{ee} \end{bmatrix}, \quad B_u = \begin{bmatrix} B_u^e & B_u^i \end{bmatrix}, \quad B_v = \begin{bmatrix} B_v^i & B_v^e \end{bmatrix}.$$

Introduce also a square matrix \bar{I} that has ones on the diagonal perpendicular to the main diagonal and zeroes everywhere else. Then the matrices H, K, L in Eq. (67) are defined as

$$H = \begin{bmatrix} A_u^{ee} & 0 \\ 0 & A_v^{ee} \end{bmatrix}, \quad K = \begin{bmatrix} A_u^{ii} & \bar{I} & -(B_u^i)^T & 0 \\ & A_v^{ii} & 0 & -(B_v^i)^T \\ & & 0 & 0 \\ & & & 0 \end{bmatrix}, \quad L = \begin{bmatrix} A_u^{ie} & 0 \\ 0 & A_v^{ie} \\ B_u^e & 0 \\ 0 & B_v^e \end{bmatrix}.$$

Finally, the extra sign in Eq. (67) takes into account the difference between the order of integrations in Eqs. (66,67). Summarizing, Eq. (67) together with the Gaussian integration formulas Eqs. (13,14) allow one to write down the canonical generating function for the contracted tensor $T_{u \star v}$.

References

- [1] I. Markov and Y. Shi, "Simulating quantum computation by contracting tensor networks", arXiv:quant-ph/0511069.
- [2] F. Verstraete and J. Cirac, "Renormalization algorithms for Quantum-Many Body Systems in two and higher dimensions", arXiv:cond-mat/0407066.
- [3] Y. Shi, L. Duan, and G. Vidal, "Classical simulation of quantum many-body systems with a tree tensor network", Phys. Rev. A 74, 022320 (2006).

- [4] A. Sandvik and G. Vidal, “*Variational quantum Monte Carlo simulations with tensor-network states*”, arXiv:0708.2232.
- [5] M. Levin and C. Nave, “*Tensor renormalization group and the solution of classical lattice models*”, arXiv:cond-mat/0611687.
- [6] M. Schwartz and J. Bruck, “*Constrained codes as networks of relations*”, Proc. of IEEE ISIT2007, pp. 1386-1390 (2007).
- [7] M. E. Fisher, “*Statistical Mechanics of Dimers on a Plane Lattice*”, Phys. Rev. **124**, p. 1664 (1961).
- [8] P. Kasteleyn, “*The Statistics of dimers on a lattice*”, Physica **27**, p. 1209 (1961).
- [9] H. Temperley and M. Fisher, “*Dimer problems in statistical mechanics — an exact result*”, Philosophical Magazine **6**, p. 1061 (1961).
- [10] F. Barahona, “*On the computational complexity of Ising spin glass models*”, J. Phys. A: Math. Gen. **15**, 3241 (1982).
- [11] A. Galluccio and M. Loebl, “*A Theory of Pfaffian Orientations I*”, Electronic J. Combin. **6**, p. 1 (1999).
- [12] R. Zecchina, “*Counting over non-planar graphs*”, Physica A: Statistical Mechanics and its Applications, Vol. 302, pp. 100-109 (2001).
- [13] D. Cimasoni and N. Reshetikhin, “*Dimers on surface graphs and spin structures. I*”, arXiv:math-ph/0608070.
- [14] L. G. Valiant, “*Quantum Circuits That Can Be Simulated Classically in Polynomial Time*”, SIAM J. Comput. **31**, No. 4, p. 1229 (2002).
- [15] L. G. Valiant, “*Holographic algorithms*”, Proceedings of FOCS 04, pp. 306-315.
- [16] J.-Y. Cai and V. Choudhary, “*Valiant’s Holant Theorem and Matchgate Tensors*”, Lecture Notes in Computer Science, Vol. 3959, pp. 248-261 (2006).
- [17] J.-Y. Cai and V. Choudhary, “*On the theory of matchgate computations*”, ECCC TR06-018 (2006).
- [18] J.-Y. Cai and V. Choudhary, “*Some results on matchgates and holographic algorithms*”, ECCC TR06-018 (2006).
- [19] S. Bravyi, “*Lagrangian representation for fermionic linear optics*”, Quantum Inf. and Comp., Vol. 5, No. 3, pp.216-238 (2005).
- [20] M. Mahajan, P. Subramanya, and V. Vinay, “*A Combinatorial Algorithm for Pfaffians*”, ECCC TR99-030 (1999).
- [21] C. Itzykson and J.-M. Drouffe, “*Statistical Field Theory: Volume 1*”, Cambridge University Press, Cambridge and New York (1989).
- [22] M. Fürer and B. Raghavachari, “*Contracting planar graphs efficiently in parallel*”, Lecture Notes in Computer Science, Vol. 560, pp. 319-335 (1991).
- [23] B. Zumino, “*Normal forms of complex matrices*”, J. Math. Phys. **3**, p. 1055 (1962).
- [24] R. Diestel, “*Graph Theory*”, Graduate Texts in Mathematics, Springer-Verlag, New York (1997).

IBM T.J. WATSON RESEARCH CENTER,, YORKTOWN HEIGHTS, NY 10598
E-mail address: sbravyi@us.ibm.com

This page intentionally left blank

Probing topological order in quantum Hall states using entanglement calculations

Masudul Haque

ABSTRACT. I provide the background and a brief review of the interdisciplinary use of entanglement calculations to investigate a type of unconventional order in many-body systems, known as topological order. The discussion focuses on a particular class of topologically ordered states: the fractional quantum Hall states

1. Introduction

Given the richness of ‘emergent’ phenomena in many-particle systems, it is perhaps no surprise that some quantum many-particle states continue to resist the methods of analysis that condensed matter theory has developed till now. Important examples are *topologically ordered* states [2] and *non-Fermi liquid* states. New methods and tools are therefore essential in understanding such states and phenomena. In an unexpected twist, concepts from a completely different and much younger field, quantum information theory, are proving to be useful in this regard. In this brief review we will focus on the use of entanglement measures from quantum information to study topological order. An entanglement measure known as the *entanglement entropy*, when calculated for judiciously chosen bipartitions of the topologically ordered state, provides a physically significant topological quantum number associated with the state. Currently, topological order is receiving intense attention due to *quantum computation* proposals based on the phenomenon [1]; a novel probe for such order is an important and timely development.

We will describe entanglement calculations in the most prominent type of topologically ordered state, namely, fractional quantum Hall states.

2. Topological order and quantum Hall states

Over half a century, condensed matter theory has developed a mature, widely used, paradigm for understanding many-particle phases and phase transitions between them — using symmetries to distinguish between phases and correlation functions to characterize them. However, some states of matter continue to defy the conventional description. One important example is topologically ordered states

1991 *Mathematics Subject Classification.* 81V70, 82B10, 82B26, 81Q99.

Key words and phrases. Quantum entanglement, Topological order, Phase transitions, Topological entanglement entropy.

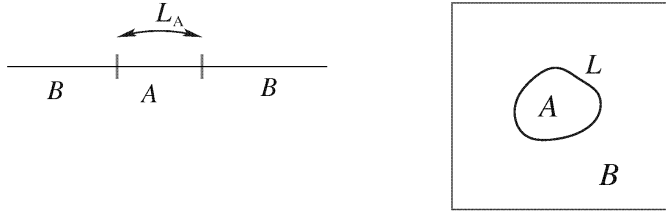


FIGURE 1. Partitioning of many-particle systems into blocks A and B , between which the entanglement (S_A) is calculated. Entanglement S_A is studied as function of boundary length L , in the asymptotic limit $L \rightarrow \infty$. *Left*: Block partitioning in 1D. Asymptotic behavior distinguishes between gapless and gapped states. For *critical* states, asymptotics gives central charge of conformal field theory [15]. *Right*: Block partitioning in 2D, relevant to the topologically ordered states.

[2], which are notoriously difficult to describe within the standard ‘Landau’ paradigm.

Topologically ordered states are ‘gapped’ in their low-energy excitation spectrum, and are further characterized by *ground-state degeneracy* on higher-genus surfaces, and in some cases by *fractionalized excitations*. For example, on a genus- g surface, the Laughlin state at filling $\nu = 1/m$ has m^g ground states. The topology-dependent degeneracy is intimately connected to fractionalization [3].

The two physical contexts for topological order are frustrated magnet systems and quantum Hall systems. In the magnetic context, topological order remains a theoretical prospect, as there are no experimental realizations. A number of topologically ordered magnetic states have been constructed theoretically; *e.g.*, (1) Kitaev’s models [4]; (2) quantum dimer models [5] on non-bipartite lattices [6]; (3) the *chiral spin liquid* of Laughlin and Kalmeyer [7]; (4) spin liquid states obtained by Gutzwiller-projecting BCS states [8].

The only confirmed *experimental* realizations of topological order are the fractional quantum Hall (FQH) states occurring in two-dimensional (2D) electrons in a magnetic field [9, 2]. Realizations of FQH states have also been proposed in cold-atom setups [10]. FQH states have long fascinated the condensed-matter community due to their remarkable transport properties and the exotic nature of their quasiparticle excitations. Recently there has been enhanced interest in FQH states with *non-abelian statistics* [11, 12, 13], due to the possibility of implementing quantum computation schemes topologically protected from decoherence [1]. The unusual features of FQH states have been notoriously difficult to characterize using traditional condensed-matter concepts such as local order parameters and n -point correlation functions. In this review we will focus on an alternate characterization of FQH states, via a recent connection found between topological order and entanglement entropy.

3. Entanglement entropy in condensed matter

The entanglement entropy is one of several possible measures of bi-partite quantum entanglement between partitions A and B of a quantum state. It is defined

as $S_A = -\text{tr}[\rho_A \ln \rho_A]$, in terms of the reduced density matrix $\rho_A = \text{tr}_B \rho$ obtained by tracing out B degrees of freedom from the system density matrix ρ . If A and B are two spins (qubits), one finds $S_A = 0$ for *product states* like $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, and in contrast $S_A \neq 0$ for *entangled states* such as $(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$ or $(c_1 |\uparrow\uparrow\rangle + c_2 |\downarrow\downarrow\rangle)$.

In the original (quantum information) setting, partitioning is often obvious: A and B can be just two qubits or two qutrits. For a many-particle system, there are exponentially many ways of partitioning. A challenge is to decide which partitioning will lead to physically interesting information. One prominent example is the study of the entanglement between a block (A) and the rest (B) of a many-particle system, measured by the entanglement entropy S_A , as a function of the block size (Fig. 1). For such *block partitioning* of many-particle ground states, the general rule (‘area law’) is that the entanglement entropy scales as the size of the boundary between the A and B blocks [14, 15]. Subtle information about the nature of the many-particle state can be contained in the coefficients, logarithmic corrections, or subleading terms in this basic relationship. For one-dimensional (1D) systems, the asymptotic behavior of S_A (Fig. 1 left) provides a distinction between *gapless* and *gapped* states, a result widely known and well-exploited by now [15]. More recently, and more pertinent to this review, the block entanglement entropy is also showing promise for exploring unconventional states in two dimensions (Fig. 1 right), such as topologically ordered states [16, 17].

4. The topological entanglement entropy

For topologically ordered states in two dimensions, the following theorem has been presented recently [16, 17]. If L is the length of the boundary between the two blocks (*e.g.*, Fig. 1 right), the entanglement entropy in the large- L limit scales as

$$S_A = \alpha L - \gamma + \mathcal{O}(L^{-1}).$$

As usual the scaling relationship applies to situations where A is large and the total system is infinite. The subleading term γ is called the *topological entanglement entropy*. This quantity is the logarithm of the so-called *total quantum dimension* of the topological field theory describing the topological order of the state. The total quantum dimension \mathcal{D} is given by $\mathcal{D} = (\sum_i d_i^2)^{1/2}$, where the d_i ’s are the quantum dimensions of the individual sectors making up the topological field theory. These individual quantum dimensions are set by fusion rules of the fundamental anyons in the field theory, as illustrated in Sec. 5 by examples in the FQH context.

After the concept was introduced [16, 17], the topological entanglement entropy has been calculated for several topologically ordered systems, notably quantum dimer models [18], Kitaev models [19, 20], and FQH systems [21, 22, 23].

5. Topological entanglement entropy for fractional quantum Hall systems

The topological field theory for a $\nu = 1/m$ Laughlin state has a fundamental anyon (of fractional charge $1/m$), which generates m abelian sectors. The quantum dimension is unity in all sectors ($d_i = 1$). Thus for the $\nu = 1/m$ abelian Laughlin state, the total quantum dimension is $\mathcal{D} = \sqrt{m}$ and the topological entanglement entropy is $\gamma = \ln \sqrt{m}$. For $m = 3$ this gives $\gamma = \frac{1}{2} \ln 3 \simeq 0.55$.

The situation is more interesting for states with non-abelian quasiparticles, because some anyon sectors now contribute $d_i > 1$. Some examples have been

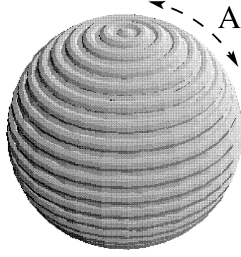


FIGURE 2. Spherical geometry for finite-size FQH calculations; partitioning into regions A and rest (B).

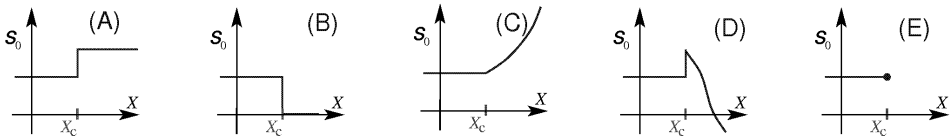


FIGURE 3. Intercept of block entropy $S_A(L)$ at phase transition. The $X < X_c$ region is a topologically ordered phase.

detailed in Refs. [16, 24, 22]. In particular, for the $m = 2$ Moore-Read state, there are six sectors, two each of quasiparticles denoted by I , σ , ψ . These contribute $d_I = 1$, $d_\sigma = \sqrt{2}$, $d_\psi = 1$, leading to $\mathcal{D} = \sqrt{8}$ and $\gamma = \ln \sqrt{8} \simeq 1.04$. The non-abelian nature shows up in the fact that γ is larger than $\ln \sqrt{6}$, which would be expected if there were six merely abelian sectors.

5.1. Explicit calculations. Extracting the topological entanglement entropy γ explicitly from quantum Hall wavefunctions is a complicated problem. Numerically, this has been done in Refs. [21, 22] for explicitly constructed Laughlin [9] and Moore-Read [11] states, and in Ref. [23] for the ground states of Coulomb Hamiltonians at appropriate filling.

When working with finite-size FQH wavefunctions, one has to make a choice of geometry, generally avoiding systems with boundaries. (FQH states have nontrivial edge effects.) The common choices are spherical and toroidal geometries, used respectively in Refs. [21, 22] and in Ref. [23]. In each case, the finite-size numerical data has to be extrapolated to the thermodynamic limit. The spherical geometry (used in Refs. [21, 22]) involves magnetic orbitals shaped as “lines of latitude” [25, 26]. Fig. 2 shows the choice of partition A used in Refs. [21, 22]. Using entanglement data for this type of partitioning in finite-size FQH wavefunctions, γ can be extracted after extrapolation to the macroscopic limit. Extrapolation remains a tricky issue and improvements are being developed compared to the methods used in Refs. [21, 22].

5.2. Prospective uses. The successful explicit calculation of the topological entanglement entropy γ for model states and Coulomb ground states [21, 22, 23] opens up the exciting possibility of using γ as a novel tool to study quantum Hall physics. Prospective uses are outlined below.

First, one can hope to use entanglement calculations to probe quantum phase transitions between FQH and non-FQH ground states. For the block entanglement

entropy, let us imagine that we have determined the asymptotic relationship

$$S_{(L \rightarrow \infty)} \longrightarrow \alpha L - s_0$$

where L is the boundary of the block. Note that this is not necessarily always possible; in some 2D phases the leading term might not be purely linear.

In a topologically ordered phase, the negative intercept s_0 will by definition be equal to the topological entropy, $\gamma = \ln \mathcal{D}$. Fig. 3 shows what can happen to s_0 as the 2D system is driven across a quantum phase transition away from the topologically ordered state, by varying a parameter X across the critical value X_c . In the parameter range $X < X_c$ where the system is in the topologically ordered phase, s_0 is fixed at a positive plateau ($s_0 = \gamma$).

Case A shows a transition into another topologically ordered state with a different quantum dimension; s_0 jumps to another constant value γ' . The other figures show transitions to non-topological phases. Case B shows a transition to a gapped state which is not topologically ordered – the intercept drops to zero. Cases C and D show continuous and discontinuous transitions into non-topological phases, in which the negative intercept is nonzero but not constant. Finally, Case E shows a transition into a state where the leading term in the asymptotic behavior of $S_A(L)$ is not linear, so that s_0 as is undefined.

A second exciting prospect is to use γ calculations to test which conformal field theories are appropriate for certain states. There are FQH states (*e.g.*, composite fermion states) for which the underlying field theory is not clear. Since γ is related to the quantum dimensions (d_i) of the theory, such determination of γ would place strong bounds on acceptable conformal field theories.

Finally, for quantum Hall fractions at which there are more than one candidate theoretical state, γ calculations could be used to distinguish between proposed candidate states if they have different total quantum dimension.

References

- [1] M. Freedman, M. Larsen, and Z. Wang; Commun. Math. Phys. **227**, 605 (2002). L. B. Ioffe *et. al.*; Nature **415**, 503 (2002). S. Das Sarma, M. Freedman, and C. Nayak; Phys. Rev. Lett. **94**, 166802 (2005); also *Physics Today*, July 2006, p. 32. A. Yu. Kitaev, Ann. Phys. **303**, 2 (2003). S. Das Sarma *et. al.*, arXiv:0707.1889.
- [2] X. G. Wen & Q. Niu; Phys. Rev. B **41**, 9377 (1990).
X. G. Wen, Phys. Rev. B **40**, 7387 (1989); J. Math. Phys. **4**, 239 (1990).
X. G. Wen; *Quantum Field Theory of Many-body Systems*, Oxford, 2004.
- [3] Oshikawa & Senthil; Phys. Rev. Lett. **96**, 060601 (2006).
- [4] A. Yu. Kitaev; Ann. Phys. **303**, 2 (2003); Ann. Phys. **321**, 2 (2006).
- [5] S. A. Kivelson, D. S. Rokhsar, and J. P. Sethna, Phys. Rev. B **35**, 8865 (1987).
D. S. Rokhsar and S. A. Kivelson, Phys. Rev. Lett. **61**, 2376 (1998).
- [6] D. S. Rokhsar and S. A. Kivelson, Phys. Rev. Lett. **61**, 2376 (1998). R. Moessner and S. L. Sondhi, Phys. Rev. Lett. **86**, 1881 (2001). G. Misguich, D. Serban, and V. Pasquier, Phys. Rev. Lett. **89**, 137202 (2002).
- [7] V. Kalmeyer and R. B. Laughlin; Phys. Rev. Lett. **59**, 2095 (1987); Phys. Rev. B **39**, 11879 (1989). R. B. Laughlin, Ann. Phys. (N.Y.) **191**, 163 (1989). R. B. Laughlin and Z. Zou, Phys. Rev. B **41**, 664 (1990).
- [8] D. A. Ivanov and T. Senthil, Phys. Rev. B **66**, 115111 (2002).
Paramekanti *et. al.*, Phys. Rev. B **71**, 094421 (2005).
- [9] D. C. Tsui, H. L. Stormer, and A. C. Gossard; Phys. Rev. Lett. **48**, 1559 (1982). R. B. Laughlin; *ibid.* **50**, 1395 (1983).
- [10] N. K. Wilkin, J. M. F. Gunn, and R. A. Smith, Phys. Rev. Lett. **80**, 2265 (1998). N. R. Cooper and N. K. Wilkin, Phys. Rev. B **60**, R16279 (1999). N. Regnault and Th. Jolicoeur, Phys.

- Rev. B **70** 241307 (2004). A. S. Sorenson, E. Demler, and M. D. Lukin; Phys. Rev. Lett. **94**, 086803 (2005).
- [11] G. Moore and N. Read, Nucl. Phys. B**360**, 362 (1991).
 - [12] N. Read and E. Rezayi, Phys. Rev. B **59**, 8084 (1999).
 - [13] E. Ardonne and K. Schoutens, Phys. Rev. Lett. **82**, 5096 (1999).
 - [14] M. Srednicki, Phys. Rev. Lett. **71**, 666 (1993).
 - [15] G. Vidal, J. I. Latorre, E. Rico and A. Kitaev, Phys. Rev. Lett. **90**, 2279021 (2003). V.E. Korepin; Phys. Rev. Lett. **92**, 096402 (2004). P. Calabrese and J. Cardy; J. Stat. Mech. **0406**, 002 (2004).
 - [16] A. Kitaev & J. Preskill; Phys. Rev. Lett. **96**, 110404 (2006).
 - [17] M. Levin & X. G. Wen; *ibid.* **96**, 110405 (2006).
 - [18] S. Furukawa & G. Misguich; Phys. Rev. B **75**, 214407 (2007).
 - [19] C. Castelnovo and C. Chamon, Phys. Rev. B **76**, 184442 (2007).
 - [20] C. Castelnovo and C. Chamon, Phys. Rev. B **77**, 054433 (2008).
 - [21] M. Haque, O. Zozulya and K. Schoutens; Phys. Rev. Lett. **98**, 060401 (2007).
 - [22] O. S. Zozulya, M. Haque, K. Schoutens, and E. H. Rezayi; Phys. Rev. B **76**, 125310 (2007).
 - [23] B.A. Friedman and G. C. Levine, eprint arXiv:0710.4071.
 - [24] P. Fendley, M. P. A. Fisher, and C. Nayak, J. Stat. Phys. **126**, 1111 (2007).
 - [25] F. D. M. Haldane, Phys. Rev. Lett. **51**, 605 (1983).
 - [26] D. P. Arovas, A. Auerbach, and F. D. M. Haldane, Phys. Rev. Lett. **60**, 531 (1988).

MAX-PLANCK INSTITUTE FOR THE PHYSICS OF COMPLEX SYSTEMS, NÖTHNITZERSTR. 38,
01187 DRESDEN, GERMANY

E-mail address: `haque@mpipks-dresden.mpg.de`

Topological Order and Entanglement

Alioscia Hamma

ABSTRACT. We show the connection between Topological Order and Quantum Entanglement. Quantum many-body systems can organize themselves in an order that cannot be explained by local order parameters and breaking of local symmetries. In a finite system, this corresponds to lattice gauge theories. It is shown that quantum entanglement can serve as an order parameter, being a non local quantity. Topologically ordered states have a pattern of entanglement that is peculiar. Group-theoretic and numerical methods are used to compute entanglement from the topologically ordered state through the quantum phase transition to a polarized state.

For many years, the paradigm of condensed matter theory has been the Landau's theory of symmetry breaking. According to this theory, phases of the matter are described by the symmetries of their ground state, and phase transitions are explained in terms of symmetry breaking [1]. Then, the fractional quantum Hall effect was discovered. The phenomenon occurs in a two dimensional electron gas, subject to an orthogonal very strong ($\sim 1T$) magnetic field, and at very low ($\sim 30mK$) temperature. What is important here, is that different fractional quantum Hall liquids corresponding to different filling factor ν have exactly the same symmetries and cannot thus be characterized in terms of Landau's theory. So in nature there are states of the matter whose internal order is not described by symmetry. They are, in fact, *topologically ordered*. Topological order is a novel description of the order in the matter [4]. In fractional quantum Hall states, it is revealed in the robust degeneracy of the ground state. This degeneracy depends on the topology of the compact space. For instance, if we build the system on a compact surface of genus g , and for a filling factor $\nu = 1/q$, the ground state is q^g -fold degenerate. In presence of defects or perturbations, the degeneracy is lifted in a way that is exponentially suppressed in the size of the system [5]. The robustness of such degeneracy, against arbitrary perturbations, is at the root of Topological Quantum Computation [8, 6]. If the degeneracy is robust, then it is possible to encode information in the ground state manifold in a way that is fault tolerant. Also the operations performed in that subspace will be fault tolerant. Error correction will be self implemented at the physical level [6].

Models for Topological Quantum Computation are models with spins on a lattice. The simplest of these models is the one invented by Kitaev in his remarkable

1991 *Mathematics Subject Classification.* 81T25, 81T45, 94A17.

Key words and phrases. Topological Order, Quantum Entanglement, Quantum Information, Quantum Phase Transitions.

paper on the toric code [6]. Topological order emerges from an underlying effective local gauge theory. In the simplest example, we find the simplest discrete gauge theory: Z_2 . This means that the ground state (and all low energy states) are invariant under Z_2 local gauge transformations. It has been known since the beginning of lattice gauge theories that then no local order parameter is possible [17]. So we have a phase of the matter, that cannot be described by a local order parameter. This is another way to say that the symmetry description of Landau does not work here. On the other hand, if we place a very strong magnetic field -say along the z direction - on every spin, the system will polarize and the expectation value of the magnetic field in the z direction will be not vanishing. So now we ask ourselves: what is the the order parameter for the topological phase? One possibility is given by the expectation value of Wilson loops. At $T = 0$, Wilson loops are good observables (because they are gauge invariant), and are not local, so they could characterize the topologically ordered phase. It turns out, that the ground state $|\Psi_0\rangle$ of the toric code is such that

$$(1) \quad \langle \Psi_0 | W[\gamma] | \Psi_0 \rangle = 1$$

where $W[\gamma]$ is a Wilson loop based on the closed curve γ of arbitrary length. We will see that this corresponds to the phenomenon of (closed) string condensation. We remark that at $T > 0$, when open strings are present, Wilson loops have expectation value zero and are completely useless.

In this paper, we want to explore what we believe is a richer way to characterize and describe topological order. We will show the connection between topological order and quantum entanglement. Quantum entanglement is one of the most important features of quantum mechanics, and it has been extensively used in quantum information theory. Quantum entanglement in a bipartite state $|\Psi_0\rangle$ is measured by the von Neumann entropy. We first decide a bipartition of the Hilbert space: $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. For instance, if we have spins on a lattice, we can bipartite the lattice itself in two regions A and B and split the Hilbert space accordingly. Then we first compute the reduced density matrix obtained by tracing out all the degrees of freedom in \mathcal{H}_B :

$$(2) \quad \rho_A = \text{Tr} |\Psi_0\rangle \langle \Psi_0|$$

If the state is not separable, the matrix ρ_A will be a mixed state. We can thus compute its entropy by

$$(3) \quad S = -\text{Tr} (\rho_A \log \rho_A)$$

This is the von Neumann entropy as measure of entanglement.

Now let us examine the toric code [6]. We start with a square lattice \mathcal{R} on a torus and place spin-1/2 on its links. If we have n spins, the Hilbert space will be $\mathcal{H} = \text{span}\{|0\rangle, |1\rangle\}^{\otimes n}$, in the σ^z basis. Now to every site s in the lattice we can consider the product $A_s = \otimes_{j \in s} \sigma_j^x$ over all the links connected to s . Similarly, for every plaquette p , we define the operator $B_p = \otimes_{j \in \partial p} \sigma_j^z$ acting on all spins along the boundary of p .

The model is therefore given by the Hamiltonian

$$(4) \quad H = -\lambda_A \sum_s A_s - \lambda_B \sum_p B_p - \xi \sum_j \sigma_j^z$$

the toric code corresponds to the model in absence of the external magnetic field, i.e., $\xi = 0$. In the limit of $\lambda_B \gg \lambda_A, \xi$ the model realizes an effective Z_2 gauge

theory. This is because one can see $\psi' = B_p \psi$ like a Z_2 gauge transformation. Therefore all the states with low energy will obey to the constraint $B_p \psi = \psi$. The low energy sector of the theory corresponds to the gauge invariant space of the gauge theory. Since all the operators A_s and B_p commute, we can easily find the ground state of the toric code by implementing all the local constraints $A_s \Psi_0 = B_p \Psi_0 = \Psi_0$. We do that by starting from a gauge invariant state like the spin polarized state $|\text{vac}\rangle = \otimes_{i=1}^n |0\rangle_i$ and projecting down the subspaces of all the constraints given by the A_s . The ground state will thus be given by

$$(5) \quad |\Psi_0\rangle = |\overline{X}|^{-\frac{1}{2}} \sum_{x \in \overline{X}} x |\text{vac}\rangle$$

where \overline{X} is the group generated by the set of all the A_s . Because of the global constraint $\prod_{s \in \mathcal{R}} A_s = I$, the order of the total group \overline{X} is $|\overline{X}| = 2^{\frac{n}{2}-1}$. The constraint comes from the fact that every A_s is idempotent, which is a consequence of the Z_2 local gauge structure.

We say that every time we flip a spin from $|0\rangle$ to $|1\rangle$ we have drawn a little "string" on the lattice. So now we see that $|\text{vac}\rangle$ is the vacuum of the strings and that the A_s act on the vacuum by creating a small loop that intersects the four spins flipped. Moreover, the product of stars creates bigger (contractible) loops. So we can see that the ground state $|\Psi_0\rangle$ is the uniform superposition of all the possible products of closed (contractible) strings of any length. Now consider the two non contractible loops around the torus, and let us call them t_1, t_2 . We also see that if we act with t_1 or t_2 around the torus over the state $|\Psi_0\rangle$, we obtain an orthogonal state that is still a ground state. This is because all loops, no matter if contractible or not, commute with the Hamiltonian. Therefore the ground state manifold is given by

$$(6) \quad \mathcal{L} = \text{span}\{|\overline{X}|^{-\frac{1}{2}} (t_1)^i (t_2)^j \sum_{x \in \overline{X}} x |\text{vac}\rangle; i, j \in \{0, 1\}\},$$

which is fourfold degenerate [14]. On a lattice on a Riemann surface of genus g , there are $2g$ incontractible loops $\{t_j\}_{j=1}^{2g}$, and therefore \mathcal{L} is 2^{2g} -fold degenerate [6, 16]. The degeneracy of the ground state depends on the topology of the compactified space.

Now we can also see by direct computation why there is string condensation and Eq.(1) holds for every closed string or product of them. Another very special feature of topological order is the following. Consider a region A of the lattice and the reduced density matrix ρ_A^0 and ρ_A^1 associated to it for the two states $|\Psi_0\rangle, t_1 |\Psi_0\rangle$. Now, despite the fact that these two states are perfectly distinguishable - in fact, they are orthogonal - they are locally identical: $\rho_A^0 = \rho_A^1$. Finally, we see that local order parameters are not possible. It is easy to see for instance that $\langle \Psi | \sigma_i^z | \Psi \rangle = 0$ for every $\Psi \in \mathcal{L}$.

Now we proceed to understand the entanglement in this ground state. Since this state is described by a superposition over elements of a group, we use the following technique. Define the local subgroups of \overline{X} with respect to the regions A, B :

$$(7) \quad X_A = \{x \in \overline{X} | x = x_A \otimes I_B\}$$

$$(8) \quad X_B = \{x \in \overline{X} | x = I_A \otimes x_B\}$$

Then we want to define the group obtained by modding out the two local parts:

$$(9) \quad X_{AB} = \frac{\overline{X}}{X_A \cdot X_B}$$

Every element x in \overline{X} then can be written like $x = (x_A \otimes x_B)h$ with $x_A \otimes I_B \in X_A, I_A \otimes x_B \in X_B, [h] \in X_{AB}$. Then, consider the more general case of a state where the superposition is not uniform:

$$(10) \quad |\phi\rangle = \sum_{x \in \overline{X}} \alpha(x) x |vac\rangle$$

then we have the following theorem [7]:

Theorem. *If the coefficients $\alpha(x)$ in Eq.(10) respect the separability condition $\alpha(x) = \alpha_A(x_A)\alpha_B(x_B)\beta(h)$, then the von Neumann entropy in the state Eq.(10) is given by $S(|\phi\rangle) = -\sum_{[h] \in X_{AB}} |\beta(h)|^2 \log |\beta(h)|^2$. In the case of a more generic group G such that it is not true that $\langle vac|g|vac\rangle = 0$ for any $g \in G$, then we only get an upper bound to S .*

There are some important consequences of this formula [15, 16]. First, we have the corollary:

Corollary 1. $G = G_A \cdot G_B \Rightarrow S(|\phi\rangle) = 0$ So if and only if for some system we find a bipartition such that G is just the product of the local parts, the entanglement for that bipartition is zero. The interesting thing is that for topologically ordered systems this is never true:

Corollary 1b. *For a topologically ordered system, $G \neq G_A \cdot G_B$ for every bipartition (about the degrees of freedom on the links) of the Hilbert space. Hence, the system is always entangled.*

The second, very important consequence, stems from the following:

Corollary 2. $S(|\phi\rangle) \leq \log |G_{AB}|$ Which means that for the case of the group of strings, the exact entanglement is given by the formula $S(|\phi\rangle) = \log |X_{AB}|$

Corollary 2 not only gives us an exact formula for the entanglement. It also has a very important geometric interpretation, that leads to an important characterization of topological order. The group X_{AB} is generated by the operators A_s in some set L_{AB} , it turns out that $S = |L_{AB}|$, that is the number of independent A_s operators that generate the non local group. As we saw above, the gauge structure implies that not all the A_s are independent and this implies [15, 16] that the set L_{AB} must therefore be made of all those A_s that act on both \mathcal{H}_A and \mathcal{H}_B , minus 1. If the region A has a boundary of length L that is regular enough, it is easy to see that the number of elements in L_{AB} is thus $L - 1$:

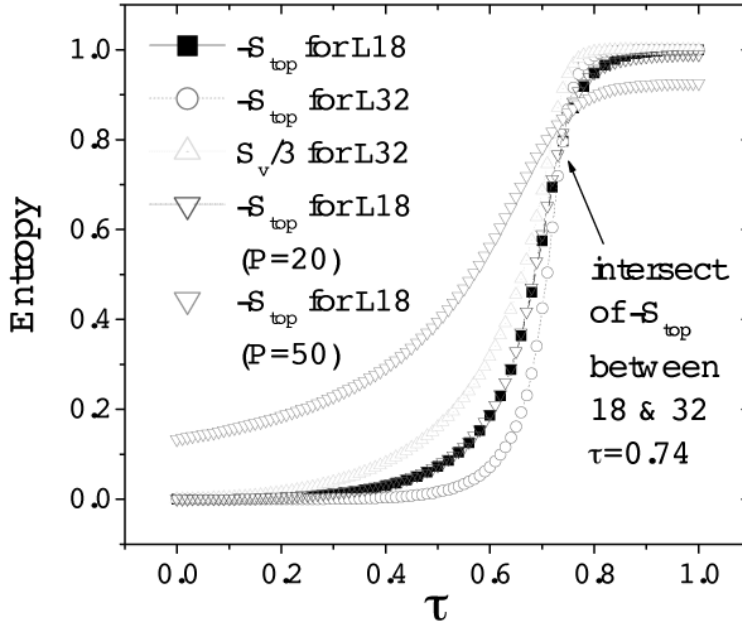
Proposition. *For a regular region A such that its boundary has length L , the entanglement entropy in the ground state of the toric code is given by $S = L - 1$.*

The correction -1 to the boundary law for the entanglement entropy is due to the topological order of the toric code [15, 16]. The situation is entirely general: every topologically ordered state has a finite correction γ to the boundary law that depends on the underlying local gauge theory [13]. The finite correction γ has been called *Topological Entropy*, S_{top} . It is important to realize that in a non topologically ordered state the term γ would vanish, as it was argued in [13]. *Therefore the (highly non local) pattern of quantum entanglement characterizes topological order.* Note that for a disconnected region, the correction γ depends on the number of disconnected regions, as it was argued in [19].

So now let us turn our attention to the transition to topological order, and how topological entropy appears. In the model Eq.(4), there are two phases depending on the ratio λ_A/ξ . When $\xi \gg \lambda_A$, the external magnetic field is dominant, and all the spins align in the positive z -direction. The ground state is completely polarized. When instead $\xi \ll \lambda_A$, we expect to be in the topologically ordered phase, with a topological entropy $S_{top} = 1$. In order to do so, we can set $\xi = 1 - \tau$ and $\lambda_A = \tau$ and study the resulting model $H(\tau)$ for every value of $\tau \in [0, 1]$. In [9], it was argued that the adiabatic evolution from the spin polarized ground state $\Psi_0(\tau = 0)$ to the topologically ordered ground state of the toric code $\Psi_0(\tau = 1)$ of Eq.(5) can happen in a time scaling like $T = O[\sqrt{n}]$ and that the adiabatic evolution does not mix the ground states belonging to different topological sectors of Eq.(6), even in presence of random arbitrary perturbations. In the thermodynamical limit, $T \rightarrow \infty$, signaling a quantum phase transition between the two phases. This happens because for a critical value of $\tau_c \sim 0.73$, the system becomes gapless. The quantum phase transition can be mapped to the one of the $2D$ quantum Ising model, and therefore is of the second order, see also [21, 10].

In [18] it has been studied the model $H(\tau) + V$ numerically, where V is a random magnetic field on every spin, of strength that is $P = 20\%, 50\%$ the value of τ . The model has been exactly diagonalized for every value of τ for systems as big as 18 and 32 spins, indicated with $L18$ and $L32$ respectively. Having obtained the exact ground state $\Psi_0(\tau)$ as a function of τ , we have first computed the corresponding entanglement for a generic bipartition, showing that its derivative diverges at the quantum critical point. According to the general theory of [11], this also means that the quantum phase transition is of the second order. Also the fidelity criterion of [12] indicates the same result. Then, finally, we have computed the topological entropy $S_{top}(\tau)$. The results are shown in the Fig. below, showing S_{top} for $L18$ and $L32$, and von Neumann entropy S_v for a region A corresponding to a plaquette of spins, for $L32$, for the ideal ($V = 0$) and perturbed model. S_v assumes the value $l - 1 = 3$ in the entire TO phase, where $l - 1$ is the exact value of S_v for the pure Kitaev model ($\tau = 1$) and $l = 4$ is the length of the border of a plaquette. S_{top} is zero in the spin-polarized phase and quickly reaches unity in the TO phase. Notice that the two curves for different lattice sizes intersect at the critical point. Moreover, it shows that the topological character of the quantum phase transition and of the phases is resilient to perturbations.

To conclude, topological order is a novel and rich concept that describes exotic phases of the matter. There is still a lot to understand about the classification of topological order. Quantum entanglement characterizes topological order its topological pattern. We want to add that, unlike Wilson loops, the entanglement retains some information on topological order even at finite temperature, as it was discovered by Castelnovo and Chamon in [20]. The relationship between quantum entanglement and quantum and topological order is an exciting field of investigation, which will bring more insight in both the understanding of condensed matter and quantum information theory.



References

- [1] L.D. Landau, and E.M. Lifschitz, *Course of Theoretical Physics Vol. 5*, Pergamon, London (1958).
- [2] D.C. Tsui, H.L. Stormer, and A.C. Gossard, Phys. Rev. Lett. **48**, 1559 (1982).
- [3] R.B. Laughlin, Phys. Rev. Lett. **50**, 1395 (1983).
- [4] X.G. Wen, Phys. Rev. B **40**, 7387 (1989); Int. J. Mod. Phys. B **4**, 239 (1990); Adv. Phys. **44**, 405 (1995); *Quantum Field Theory of Many-Body Systems* (Oxford, 2004).
- [5] X.-G. Wen and Q. Niu, Phys. Rev. B **41**, 9377 (1990).
- [6] A.Y. Kitaev Annals Phys. **303**, 2 (2003).
- [7] A. Hamma, R. Ionicioiu, and P. Zanardi Phys. Rev. A **72**, 012324 (2005);
- [8] M.H. Freedman *et al.*, Bull. Amer. Math. Soc. **40**, 31 (2003).
- [9] A. Hamma, and D. Lidar, Phys. Rev. Lett. **100**, 030502 (2008).
- [10] S. Trebst *et al.*, Phys. Rev. Lett. **98**, 070602 (2007).
- [11] L.-A. Wu, M.S. Sarandy, and D.A. Lidar, Phys. Rev. Lett. **93**, 250404 (2004); L.-A. Wu *et al.*, Phys. Rev. A **74**, 052335 (2006).
- [12] P. Zanardi, and N. Paunković, Phys. Rev. E **74**, 031123 (2006).
- [13] A. Kitaev and J. Preskill, Phys. Rev. Lett. **96**, 110404 (2006); M. Levin and X.-G. Wen, Phys. Rev. Lett. **96**, 110405 (2006).
- [14] A. Hamma, P. Zanardi, and X.-G. Wen, Phys. Rev. B **72** 035307 (2005).
- [15] A. Hamma, R. Ionicioiu, and P. Zanardi, Phys. Lett. A **337**, 22 (2005).
- [16] A. Hamma, R. Ionicioiu, and P. Zanardi, Phys. Rev. A **71**, 022315 (2005).
- [17] S. Elitzur, Phys. Rev. D **12**, 3978 (1975).
- [18] A. Hamma, W. Zhang, S. Haas, D.A. Lidar, Phys. Rev. B **77**, 155111 (2008);
- [19] C. Castelnovo and C. Chamon, Phys. Rev. B **76**, 174416 (2007).
- [20] C. Castelnovo and C. Chamon, Phys. Rev. B **76**, 184442 (2007).
- [21] E. Ardonne, P. Fendley and E. Fradkin, Ann. Phys. **310**, 493 (2004).

DEPARTMENT OF CHEMISTRY, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089, USA

E-mail address: hamma@usc.edu

Hierarchical Quantum Search

Vladimir E. Korepin and Ying Xu

ABSTRACT. Database search has wide applications and is used as a subroutine in many important algorithms. In this paper we will consider a database with a single target item. Quantum algorithm [Grover] locates the target item faster than any classical algorithm. In addition to a full [Grover] search, it frequently occurs that one is looking for a group of items [a block] containing the target item, rather than the target item itself. This problem is known as partial search. As a generalization of the full search, partial search is of particular importance in practice. Partial search trades accuracy for speed, i.e. it works faster than a full search. There exists different versions of partial search. We will study the optimized version of the algorithm discovered by Grover and Radhakrishnan and call it GRK. GRK can be applied successively [in a sequence]. First the database is partitioned into blocks and GRK is applied to find the target block. Then this target block is partitioned into sub-blocks and GRK is used again to find the target sub-block. This procedure can be repeated if the database is large enough. [This sequence of GRK's is called a hierarchy.] Another possibility is to partition the database into sub-blocks directly and use GRK to find the target sub-block once. In this paper we will prove that the latter is faster [makes less queries to the oracle].

1. Introduction

Database search has many applications. Search algorithm enters as a subroutine in many important algorithms in computer sciences.[1, 2, 3] Grover discovered a quantum algorithm which searches a database faster than any classical algorithm.[4] Let's consider a database with one target item. We use number of queries to the oracle as complexity measure. The Grover algorithm finds the target item [with probability 1] in

$$(1) \quad j_{\text{full}} = \frac{\pi}{4} \sqrt{N}, \quad N \rightarrow \infty$$

iterations [queries to the oracle]. We shall call it a full search.

It occurs frequently in practice that less information is needed. For example, the address of the target item in binary form is $|t\rangle = |b_1 b_2 b_3 \dots b_n\rangle$, and we want to find only the first 3 bits $b_1 b_2 b_3$. This means that the database is partitioned into 8 blocks. All items in a block share the common feature such that the first 3 bits being the same. We want to find the block containing the target item. This is

1991 *Mathematics Subject Classification.* 81P68.

Key words and phrases. Quantum Search; Grover Algorithm; Partial Search; Hierarchical Search.

an example of partial search. The general problem of partial search considers the following: An N item database is partitioned into K blocks, each of the same size

$$(2) \quad b = \frac{N}{K}.$$

A user wants to find the block containing the target item, instead of the target item itself. The block with the target item is called the target block; others non-target blocks. Partial search naturally arises in list matching.[5] Partial search is not only a compromise on accuracy for speed, but also has its own significance. Partial search can find all items in the database which share some features with the target item. This can be considered as a special case of sorting problem. The GRK algorithm of partial search was suggested by Grover and Radhakrishnan,[6] and optimized in [7]. It takes $\sim \frac{\pi}{4}(1 - \text{coeff}(K))\sqrt{N}$ number of queries to find the target block. Here $\text{coeff}(K)$ is a finite positive number, which depends on K and has a limit when blocks are large $b \rightarrow \infty$. GRK is the most efficient partial search algorithm known in literature.[6, 8, 9, 7, 10]

GRK can be applied in a sequence [one after another], i.e. after the first GRK, the target block found can be further partitioned into sub-blocks. Then a second GRK can be applied to find the sub-block containing the target item [called the target sub-block]. We shall call the sequence of GRK's a partial search hierarchy. In hierarchical search we iterate GRK. A practical example would be: In order to find a hotel, we first look at a State map and then a town map. We shall see that the second GRK works faster than the first one. Actually, GRK can be conducted repeatedly until we find the smallest target sub-sub-block interested. The total number of queries is the sum of queries of each GRK in the hierarchy. [We use number of queries as measure of complexity.]

Alternative to a partial search hierarchy which finds the target sub-sub-block, we could partition the database directly into sub-sub-blocks and use GRK once: We shall call it direct partial search. Although each GRK works faster than the previous one in the hierarchy, it is not guaranteed that the total number of queries in the hierarchy [sequence of GRK's] is less than that of a direct partial search. On the contrary, we will prove that *direct partial search works faster*, which is the main result of the paper. For example, consider a database partitioned into 2 blocks. Each block is partitioned into 2 sub-blocks, so totally 4 sub-blocks. One could first find the target block using GRK, then the target sub-block using sequential GRK. However, it is faster to run a GRK directly over the 4 sub-blocks, which finds the target sub-block once.

The paper consists of two parts: In the first part, we start with the Grover algorithm and the GRK algorithm. Then we study the partial search hierarchy in detail. The second part proceeds to a comparison of the hierarchical partial search with direct partial search. Then we prove our main result that direct partial search works faster.

2. The Grover Search Algorithm

In our paper, we consider different methods of partial search. They are all built on the original idea of the full Grover search.[4, 2, 11] Let's formulate the problem. Consider a database of N items with one target item. ¹ The database

¹Target item also called in literature marked item or solution.

is associated with a Hilbert space with N normalized basis vectors. The basis vector corresponding to item x is denoted by $|x\rangle$. The Grover search is a quantum algorithm which starts from the uniform superposition of all basis vectors in the whole database:

$$(3) \quad |s_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle, \quad \langle s_1 | s_1 \rangle = 1.$$

The algorithm searches for a single target item $|t\rangle$ iteratively. The Grover iteration is a unitary transform:

$$(4) \quad G_1 = -I_{s_1} I_t.$$

Later we shall call it a global iteration in GRK. Here I_t and I_{s_1} are two inversions about the target item $|t\rangle$ and the uniform superposition $|s_1\rangle$ defined in (3), respectively:

$$(5) \quad I_t = \hat{I} - 2|t\rangle\langle t|,$$

$$(6) \quad I_{s_1} = \hat{I} - 2|s_1\rangle\langle s_1|,$$

where \hat{I} is the identical operator. The Grover iteration G_1 is a rotation in the Hilbert space from $|s_1\rangle$ towards the target $|t\rangle$ by an angle θ_1 defined by:[11]

$$(7) \quad \sin^2 \theta_1 = \frac{1}{N}.$$

After j_1 iterations the state of the database becomes: [11, 2]

$$(8) \quad G_1^{j_1} |s_1\rangle = \sin((2j_1 + 1)\theta_1) |t\rangle + \frac{\cos((2j_1 + 1)\theta_1)}{\sqrt{N-1}} \sum_{x \neq t}^{N-1} |x\rangle.$$

Therefore after $j_{\text{full}} = \pi/(4\theta_1) - 1/2$ iterations the probability amplitude of $|t\rangle$ becomes unity and amplitudes of other items all vanish. i.e.

$$(9) \quad G_1^{j_{\text{full}}} |s_1\rangle = |t\rangle.$$

As N becomes large $j_{\text{full}} = \pi/(4\theta_1) - 1/2$ approaches (1). More details on Grover search can be found in [2].

3. Algorithms for Partial Search

Before introducing the GRK partial search algorithm [see next section], we look at a few other algorithms for comparison:

(i) Naive Search

Pick a block randomly and make a full Grover search in it [which makes $\frac{\pi}{4} \sqrt{\frac{N}{K}}$ queries to the oracle]. If we find the target item then we understand that this is the target block. If not, then we discard this block and pick another randomly. Make a full Grover search in it and repeat this procedure till we find the target block. In the worst case the target block will be the last one. So with probability 1 we have to use

$$(10) \quad r(N, K) = \frac{(K-1)\pi}{\sqrt{K}} \frac{1}{4} \sqrt{N}$$

iterations [queries] to find the target block.²

A full Grover search finds the target item in $(\pi/4)\sqrt{N}$ queries. If we know the exact address of the target item then we also know the target block. Comparing $(\pi/4)\sqrt{N}$ with $r(N, K)$ in (10), we see that the naive version is faster only for two blocks $K = 2$. [If $K \geq 3$ a full search is faster].

(ii) Binary Search

Assume that $K = 2^k$ with k being a positive integer. Divide the database into two blocks and make a full Grover search in one block. If the target item is not found, then take the remaining block and divide it into two sub-blocks. Pick a sub-block randomly and make a full search again in it. Repeat the procedure until we are left with the last block. In the worst case, the number of queries necessary to find the target block is

$$(11) \quad \frac{\pi}{4}\sqrt{N} \left\{ \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{4}} + \dots + \frac{1}{2^{k/2}} \right\}, \quad k = \log_2 K.$$

The first two terms in the braces of (11) are greater than 1 for $K \geq 3$,

$$(12) \quad \frac{1}{\sqrt{2}} + \frac{1}{2} = \frac{\sqrt{2} + 1}{2} > 1.$$

So this algorithm is less efficient than a full Grover search, when $K > 2$.

(iii) Grover and Radhakrishnan Version

A faster version was found in [6]. Pick randomly a block and make a full Grover search in the compliment [all items in the rest of the database]. Either the target item [and block] is found after the search or the picked block is the target block. This requires $\frac{\pi}{4}\sqrt{b(K-1)} = \frac{\pi}{4}\sqrt{N}\sqrt{\frac{K-1}{K}}$ queries. It is faster than a full search.

4. The GRK Partial Search Algorithm

Grover and Radhakrishnan also discovered a faster quantum algorithm for partial search, [6] which uses the same oracle as the main Grover algorithm. [See Summary and Appendix D.] Partial search also starts from the uniform superposition of all basis states (3). A general structure of the algorithm is: [6, 12, 8, 10, 9, 7]

Step 1.: Global iterations: j_1 standard Grover iterations (4). After this step the state of database is $G_1^{j_1}|s_1\rangle$.

Step 2.: Simultaneous local iterations in each block: j_2 local Grover iterations defined in (13) below. After step 2 the state of database is $G_2^{j_2}G_1^{j_1}|s_1\rangle$.

Local iteration is defined by

$$(13) \quad G_2 = \bigoplus_{\text{blocks}}^K G_2^{\text{one}} = - \left(\bigoplus_{\text{blocks}}^K I_{s_2} \right) I_t.$$

² $(\sqrt{K}/2)(\pi/4)\sqrt{N}$ queries on average.

It is a direct sum of Grover iterations [called local queries] defined in each block

$$(14) \quad G_2^{\text{one block}} = -I_{s_2} I_t.$$

In the expression I_t is the same inversion (5), i.e. query to the oracle. I_{s_2} is a local inversion

$$(15) \quad I_{s_2} = \hat{I} - 2|s_2\rangle\langle s_2|.$$

Here $|s_2\rangle$ is the uniform superposition of items in one block

$$(16) \quad |s_2\rangle = \frac{1}{\sqrt{b}} \sum_{\text{one block}}^{\text{b items}} |x\rangle.$$

Local iteration G_2 is a the Grover iteration in each block done simultaneously in all blocks. G_2 acts trivially on non-target blocks. A non-trivial operation [rotation] is present only in the target block with new rotation angle θ_2 defined by

$$(17) \quad \sin^2 \theta_2 = \frac{K}{N} = \frac{1}{b}.$$

Note that amplitudes of all items in non-target blocks remain intact.

Step 3.: Location of the target block with a final global iteration: [8, 10, 7]

We have to vanish amplitudes of all items in non-target blocks. We can do it by application of one more global iteration. The resulting state is

$$(18) \quad |d\rangle \equiv G_1 G_2^{j_2} G_1^{j_1} |s_1\rangle = \sin \omega |t\rangle + \frac{\cos \omega}{\sqrt{b-1}} \sum_{\substack{x \neq t \\ \text{target block}}}^{\text{b-1 items}} |x\rangle.$$

The final state (18) is expressed as a superposition over items in the target block only. This is realized by requiring that the amplitude of any non-target block vanishes after the partial search, i.e.

$$(19) \quad \langle x|d\rangle = 0.$$

Here x is an arbitrary item in any non-target block. This vanishing condition can be written explicitly as an equality for j_1 and j_2 , see [7]. We shall call it a cancellation condition.

This partial search algorithm was further optimized in [7]. In the large block limit $b \rightarrow \infty$, the total number of items also large $N \rightarrow \infty$, while the ratio $K = N/b$ kept finite. Then the expression for rotation angles (7) and (17) simplifies

$$(20) \quad \theta_1 \rightarrow \frac{1}{\sqrt{N}}, \quad \theta_2 \rightarrow \frac{1}{\sqrt{b}}.$$

It turns out convenient to rewrite numbers of iterations in a scale form: [6]

$$(21) \quad j_1 = \left(\frac{\pi}{4} - \frac{\eta}{\sqrt{K}} \right) \sqrt{N}, \quad j_2 = \frac{\alpha}{\sqrt{K}} \sqrt{N}.$$

Here η and α are parameters of order 1 [they have a limit]. The ranges of these parameters are discussed in Appendix B. The vanishing condition (19) in terms of

these parameters simplifies in the large b limit: [9, 7]

$$(22) \quad \tan\left(\frac{2\eta}{\sqrt{K}}\right) = \frac{2\sqrt{K} \sin 2\alpha}{K - 4 \sin^2 \alpha}.$$

The total number of queries is

$$(23) \quad S(K) \equiv j_1 + j_2 + 1 \xrightarrow{b \rightarrow \infty} \left(\frac{\pi}{4} + \frac{\alpha - \eta}{\sqrt{K}}\right) \sqrt{N}.$$

It was minimized [subject to the constraint (22)] in [7]. The minimum number of queries is achieved at

$$(24) \quad \eta(K) = \frac{1}{2}\sqrt{K} \arctan\left(\frac{\sqrt{3K-4}}{K-2}\right), \quad \alpha(K) = \frac{1}{2} \arccos\left(\frac{K-2}{2(K-1)}\right).$$

Thus the minimized number of queries of GRK partial search [as a function of K] is

$$(25) \quad S(K) \xrightarrow{b \rightarrow \infty} \left(\frac{\pi}{4} + \frac{\alpha(K) - \eta(K)}{\sqrt{K}}\right) \sqrt{N}.$$

A proof of (24) being the minimum is given in Appendix C. Note that $\alpha - \eta$ is negative and number of blocks $K \geq 2$ in a non-trivial situation.

In the large block limit, the ω appeared in (18) is

$$(26) \quad \omega = \alpha(K),$$

see [7]. As a consequence, the state of database after GRK (18) is the following: The amplitudes of items in non-target blocks all vanish and the state of the target block is

$$(27) \quad |d\rangle = \sin \alpha(K) |t\rangle + \frac{\cos \alpha(K)}{\sqrt{b-1}} \sum_{\substack{\text{items} \\ x \neq t \\ \text{target block}}}^{b-1} |x\rangle.$$

5. The Partial Search Hierarchy

A partial search hierarchy is a sequence of GRK's. After location of the target block, we may consider a subsequent GRK partial search: The target block is further partitioned into \tilde{K} sub-blocks and we search for the sub-block containing the target item [target sub-block]. For example we can use Google Earth to find the State of New York first on the map of USA and then make a sequential search for Stony Brook in the State map.

We shall show below that a sequential GRK can be done faster than the first GRK. The coefficient $\pi/4$ in (25) is replaced by a smaller number:

$$(28) \quad \frac{\pi}{4} \rightarrow \frac{\pi}{4} - \frac{1}{4} \arccos\left(\frac{K-2}{2(K-1)}\right).$$

Each successive GRK works faster than the previous one for two reasons. First, the new database is smaller [only one block of the previous one]. Second, the initial state of the new database (27) can be represented in different forms (30) and (38) below. We see that for sequential GRK, the initial state is no longer a uniform superposition of basis vectors of the new database. It is an unevenly weighted superposition with emphasis on the target $|t\rangle$, see (30) and (38). In other words, the new initial state of the database is equivalent to a partially searched [though not

fully searched] one. This fact was studied in [7]. It was shown that after the first GRK the state of the target block [new database] can be written as [(27) rewritten]

$$(29) \quad |d\rangle = G_1 G_2^{j_2} G_1^{j_1} |s_1\rangle = \sin \alpha(K) |t\rangle + \frac{\cos \alpha(K)}{\sqrt{b-1}} \sum_{\substack{x \neq t \\ \text{target block}}}^{b-1 \text{ items}} |x\rangle.$$

We have used relation (26). Compared with (8), we see that the state after the first GRK (29) takes the form

$$(30) \quad |d\rangle = G_1 G_2^{j_2} G_1^{j_1} |s_1\rangle = G_2^{\frac{\alpha(K)}{2}} \sqrt{b} |s_2\rangle,$$

which serves as the initial state of the sequential GRK.

For notational convenience, we use a "∼" to indicate variables in sequential GRK and make the following definitions:

$$(31) \quad \text{Number of items in new database :} \quad \tilde{N} = b = \tilde{K} \tilde{b},$$

$$(32) \quad \text{Uniform superposition of new database :} \quad |\tilde{s}_1\rangle = |s_2\rangle,$$

$$(33) \quad \text{New global inversion :} \quad I_{\tilde{s}_1} = I_{s_2},$$

$$(34) \quad \text{New global iteration :} \quad \tilde{G}_1 = G_2, \quad \tilde{\theta}_1 = \theta_2,$$

$$(35) \quad \text{Uniform superposition of one sub-block :} \quad |\tilde{s}_2\rangle = \frac{1}{\sqrt{\tilde{b}}} \sum_{\substack{\text{one} \\ \text{sub-block}}}^{\tilde{b} \text{ items}} |x\rangle,$$

$$(36) \quad \text{New local inversion :} \quad I_{\tilde{s}_2} = I - 2|\tilde{s}_2\rangle\langle\tilde{s}_2|,$$

$$(37) \quad \text{New local iteration :} \quad \tilde{G}_2 = -I_{\tilde{s}_2} I_t, \quad \sin^2 \tilde{\theta}_2 = \frac{1}{\tilde{b}}.$$

Written in these notations, the initial state of new database (30) is equivalent to a partially searched one with $\frac{\alpha(K)}{2} \sqrt{\tilde{N}}$ new global queries, i.e.

$$(38) \quad |d\rangle = G_1 G_2^{j_2} G_1^{j_1} |s_1\rangle = \tilde{G}_1^{\frac{\alpha(K)}{2}} \sqrt{\tilde{N}} |\tilde{s}_1\rangle.$$

Steps of sequential GRK can be written similarly to the first GRK using new notations (31)-(37). The resultant state of target sub-block is

$$(39) \quad |\tilde{d}\rangle \equiv \tilde{G}_1 \tilde{G}_2^{\tilde{j}_2} \tilde{G}_1^{\tilde{j}_1} \left(\tilde{G}_1^{\frac{\alpha(K)}{2}} \sqrt{\tilde{N}} |\tilde{s}_1\rangle \right) = \sin \tilde{\omega} |t\rangle + \frac{\cos \tilde{\omega}}{\sqrt{\tilde{b}-1}} \sum_{\substack{x \neq t \\ \text{target sub-block}}}^{\tilde{b}-1 \text{ items}} |x\rangle.$$

Note that the vector in the parentheses is $|d\rangle$ of (27). We also have [similar to (19)]

$$(40) \quad \langle x | \tilde{d} \rangle = 0, \quad \forall x \in \{\text{items of non-target sub-blocks}\}.$$

This yields cancellation condition relating \tilde{j}_1 and \tilde{j}_2 , see [7]. We introduce parameters $\tilde{\eta}$ and $\tilde{\alpha}$ defined by

$$(41) \quad \tilde{j}_1 = \left(\frac{\pi}{4} - \frac{\alpha(K)}{2} - \frac{\tilde{\eta}}{\sqrt{\tilde{K}}} \right) \sqrt{\tilde{N}}, \quad \tilde{j}_2 = \tilde{\alpha} \sqrt{\tilde{b}}.$$

The algorithm is also optimized [7] in the large sub-block limit: $\tilde{b} \rightarrow \infty$, $\tilde{N} \equiv \tilde{K}\tilde{b} \rightarrow \infty$. In the limit, the angles (34) and (37) simplify

$$(42) \quad \tilde{\theta}_1 = \frac{1}{\sqrt{\tilde{N}}}, \quad \tilde{\theta}_2 = \frac{1}{\sqrt{\tilde{b}}}.$$

The minimum is achieved at

$$(43) \quad \begin{aligned} \tilde{\eta}(\tilde{K}) &= \frac{1}{2} \sqrt{\tilde{K}} \arctan\left(\frac{\sqrt{3\tilde{K}-4}}{\tilde{K}-2}\right) = \eta(\tilde{K}), \\ \tilde{\alpha}(\tilde{K}) &= \frac{1}{2} \arccos\left(\frac{\tilde{K}-2}{2(\tilde{K}-1)}\right) = \alpha(\tilde{K}). \end{aligned}$$

Similar to (26), we have in the large sub-block limit

$$(44) \quad \tilde{\omega} = \alpha(\tilde{K}).$$

As a result the number of queries of the sequential GRK is

$$(45) \quad \bar{S}(K, \tilde{K}) \equiv \tilde{j}_1 + \tilde{j}_2 + 1 \xrightarrow{\tilde{b} \rightarrow \infty} \left(\frac{\pi}{4} - \frac{\alpha(K)}{2} + \frac{\alpha(\tilde{K}) - \eta(\tilde{K})}{\sqrt{\tilde{K}}} \right) \sqrt{\tilde{N}}.$$

In principle, sequential GRK's can be conducted successively until the smallest target sub-sub-block is found. Here arises a question on the efficiency of hierarchical partial search, i.e. whether or not is a sequence of GRK's works faster than a direct GRK partial search of the smallest sub-sub-blocks. As will be shown in the following section, direct GRK partial search makes less queries in the quantum case.

6. Comparison of Hierarchical Partial Search with Direct Partial Search

The partial search hierarchy forms a sequence of GRK's. It starts from searching for the largest target block and ends with searching for the smallest target sub-sub-block. On the other hand, it is also possible to partition the database directly into the smallest sub-sub-blocks and use a GRK to find the target sub-sub-block in one time. One question of significance is **whether the hierarchical search works faster than the direct search or not**. This question is of practical importance and the answer turns out to be *negative*. We prove the statement by studying the first two successive GRK's in the hierarchy.

We have already derived the optimized number of queries of the first two GRK's in (25) and (45), respectively. So that the total number of queries is the sum:

$$(46) \quad \begin{aligned} T(K, \tilde{K}) &\equiv S(K) + \bar{S}(K, \tilde{K}) \\ &= \left\{ \frac{\pi}{4} + \left[\frac{\pi}{4} + \frac{1}{2} \alpha(K) - \eta(K) \right] \frac{1}{\sqrt{K}} + \left[\alpha(\tilde{K}) - \eta(\tilde{K}) \right] \frac{1}{\sqrt{K\tilde{K}}} \right\} \sqrt{N}. \end{aligned}$$

On the other hand, if the database is partitioned directly into $K\tilde{K}$ blocks, a direct GRK algorithm would require

$$(47) \quad S(K\tilde{K}) = \left[\frac{\pi}{4} + \frac{\alpha(K\tilde{K}) - \eta(K\tilde{K})}{\sqrt{K\tilde{K}}} \right] \sqrt{N}$$

queries instead. Let us compare $T(K, \tilde{K})$ and $S(K\tilde{K})$, assuming that both $K \geq 2$ and $\tilde{K} \geq 2$.

6.1. Numerical Comparison of Query Numbers and Asymptotic Analysis. Before giving the complete proof, we illustrate this fact by looking at a few concrete examples. Here in Table 6.1 we give a few numerical examples of query numbers $S(K\tilde{K})$ and $T(K, \tilde{K})$ as well as their difference, for a better understanding. It is clear that each $T - S$ is positive in the last column.

Table 1. Numerical Examples of Query Numbers.

K	\tilde{K}	$S(K\tilde{K})/\sqrt{N}$	$T(K, \tilde{K})/\sqrt{N}$	$(T(K, \tilde{K}) - S(K\tilde{K}))/\sqrt{N}$
2	2	0.61548	0.670379	0.054899
2	3	0.646015	0.695421	0.049406
3	2	0.646015	0.721158	0.075143
2	4	0.664521	0.71289	0.048369
4	2	0.664521	0.73929	0.074769
3	3	0.671394	0.741605	0.070211

Independently, when number of blocks and sub-blocks both being large, i.e. $K \rightarrow \infty$, $\tilde{K} \rightarrow \infty$, asymptotic forms of $\alpha(x)$ and $\eta(x)$ are obtained from (24) as

$$(48) \quad \alpha(x) \sim \frac{\pi}{6} + \frac{1}{2\sqrt{3}x} + \frac{5\sqrt{3}}{(6x)^2}, \quad \eta(x) \sim \frac{\sqrt{3}}{2} + \frac{1}{2\sqrt{3}x} + \frac{11\sqrt{3}}{90x^2}, \quad x \rightarrow \infty.$$

Then the query numbers (46) and (47) take asymptotic forms using (48)

$$(49) \quad S(K\tilde{K}) \sim \left\{ \frac{\pi}{4} + \left[\frac{\pi}{6} - \frac{\sqrt{3}}{2} + \frac{1}{5\sqrt{3}(2K\tilde{K})^2} \right] \frac{1}{\sqrt{K\tilde{K}}} \right\} \sqrt{N}$$

$$(50) \quad T(K, \tilde{K}) \sim \left\{ \frac{\pi}{4} + \left[\left(\frac{\pi}{3} - \frac{\sqrt{3}}{2} \right) - \frac{1}{4\sqrt{3}K} - \frac{19\sqrt{3}}{10(6K)^2} \right] \frac{1}{\sqrt{K}} + \left[\frac{\pi}{6} - \frac{\sqrt{3}}{2} + \frac{1}{5\sqrt{3}(2\tilde{K})^2} \right] \frac{1}{\sqrt{K\tilde{K}}} \right\} \sqrt{N}.$$

As for the difference (55) of query numbers, the ratio K/\tilde{K} becomes relevant in determining the asymptotic behavior. There are 3 possibilities:

If $K/\tilde{K} \rightarrow 0$, then $1/K$ is dominating, and

$$(51) \quad T(K, \tilde{K}) - S(K\tilde{K}) \sim \left[\left(\frac{\pi}{3} - \frac{\sqrt{3}}{2} \right) K^{-\frac{1}{2}} \right] \frac{1}{\sqrt{N}}.$$

If $K/\tilde{K} \rightarrow \infty$, then $1/\tilde{K}$ is dominating, and

$$(52) \quad T(K, \tilde{K}) - S(K\tilde{K}) \sim \left(\frac{1}{20\sqrt{3}} K^{-\frac{1}{2}} \tilde{K}^{-\frac{5}{2}} \right) \frac{1}{\sqrt{N}}.$$

If $K/\tilde{K} \rightarrow \text{finite number}$, then we have the same result as (51). In both the expressions (51) and (52) the coefficients of $1/\sqrt{N}$ are positive. Up to now we saw that $T > S$. Now let us formally prove as a theorem (56) that $T > S$ in general, when $K \geq 2$ and $\tilde{K} \geq 2$.

6.2. General Proof that $T(K, \tilde{K}) > S(K\tilde{K})$. Now we prove that $T(K, \tilde{K}) - S(K\tilde{K})$ is always positive in the region $K, \tilde{K} \in [2, +\infty)$. In order to complete the proof we need the following two lemmas.

LEMMA 1.

$$(53) \quad \frac{\pi}{4} + \left(\frac{1}{2} \alpha - \eta \right) (x) > 0, \quad \forall x \in [2, +\infty).$$

PROOF. $\forall x \in [2, +\infty)$

The derivative $\left[\frac{\pi}{4} + \left(\frac{1}{2}\alpha - \eta\right)\right]'(x) = \frac{1}{4\sqrt{x}}f(x)$ with $f(x) \equiv \frac{3}{\sqrt{3x-4}} - \arctan \frac{\sqrt{3x-4}}{x-2}$. While $f'(x) = \frac{-9x+8}{2x(x-1)(3x-4)^{\frac{3}{2}}} < 0$, so that $f(x)$ monotonically decreasing. Further, since that $f(2) = \frac{3}{\sqrt{2}} - \frac{\pi}{2} > 0$, $f(x) \xrightarrow{x \rightarrow +\infty} 0$, then continuous function $f(x) > 0$ in the region. [$f(x)$ is positive at one point $x = 2$ and tends to zero as x tends to infinity. As a continuous and monotonic function, $f(x)$ can never become negative nor zero in the region.] Therefore $\left[\frac{\pi}{4} + \left(\frac{1}{2}\alpha - \eta\right)\right]'(x) > 0$, so that $\frac{\pi}{4} + \left(\frac{1}{2}\alpha - \eta\right)(x)$ is a monotonically increasing function of x . With $\frac{\pi}{4} + \left(\frac{1}{2}\alpha - \eta\right)(2) = \frac{3-2\sqrt{2}}{8}\pi > 0$, we conclude that $\frac{\pi}{4} + \left(\frac{1}{2}\alpha - \eta\right)(2) > 0$ in the region. \square

LEMMA 2.

$$(54) \quad (\alpha - \eta)(x) \text{ monotonically decreasing,} \quad \forall x \in [2, +\infty).$$

PROOF. $\forall x \in [2, +\infty)$

The derivative $(\alpha - \eta)'(x) = \frac{1}{4\sqrt{x}}g(x)$ with $g(x) \equiv \frac{\sqrt{3x-4}}{x-1} - \arctan \frac{\sqrt{3x-4}}{x-2}$. While $g'(x) = \frac{1}{x(x-1)^2\sqrt{3x-4}} > 0$, so that $g(x)$ monotonically increasing. Further, since that $g(2) = \sqrt{2} - \frac{\pi}{2} < 0$, $g(x) \xrightarrow{x \rightarrow +\infty} 0$, then continuous function $g(x) < 0$ in the region. [$g(x)$ is negative at one point $x = 2$ and tends to zero as x tends to infinity. As a continuous and monotonic function, $g(x)$ can never become positive nor zero in the region.] Therefore $(\alpha - \eta)'(x) < 0$, we conclude that $(\alpha - \eta)(x)$ is a monotonically decreasing function of x in the region. \square

Having proved these two lemmas, we look at the structure of $T(K, \tilde{K}) - S(K\tilde{K})$ using (46) and (47):

$$(55) \quad T(K, \tilde{K}) - S(K\tilde{K}) = \left\{ \left[\frac{\pi}{4} + \frac{1}{2}\alpha(K) - \eta(K) \right] \frac{1}{\sqrt{K}} + \left[\left(\alpha(\tilde{K}) - \eta(\tilde{K}) \right) - \left(\alpha(K\tilde{K}) - \eta(K\tilde{K}) \right) \right] \frac{1}{\sqrt{K\tilde{K}}} \right\} \sqrt{N}.$$

Making use of **Lemma 1** (53), we see that the terms $\frac{\pi}{4} + \frac{1}{2}\alpha(K) - \eta(K)$ appearing in the first bracket of (55) is positive for $K \geq 2$. Making use of **Lemma 2** (54) and since $K\tilde{K} > \tilde{K}$, the monotonic property of $\alpha - \eta$ ensures that $\left(\alpha(\tilde{K}) - \eta(\tilde{K}) \right) > \left(\alpha(K\tilde{K}) - \eta(K\tilde{K}) \right)$. So that the second bracket of (55) is also positive for both $K \geq 2$ and $\tilde{K} \geq 2$. Therefore the whole brace of (55) is positive. As a consequence, we conclude our result in the following theorem:

THEOREM 1.

$$(56) \quad T(K, \tilde{K}) > S(K\tilde{K}), \quad \forall K, \tilde{K} \in [2, \infty).$$

i.e. Hierarchical partial search makes more queries to the oracle than direct partial search. *Direct GRK partial search works faster.*

6.3. Hierarchy with Many GRK's. Theorem (56) can be extended to the case of hierarchical search with an arbitrary number of GRK's. The direct GRK always works faster. We prove the statement as follows.

Consider a hierarchy with m GRK's. Assume that $m \geq 2$. We denote the whole operations $G_1 G_2^{j_2} G_1^{j_1}$ of each GRK by one symbol and define an operator

$$(57) \quad \mathcal{G} \equiv G_1 G_2^{j_2} G_1^{j_1}.$$

The hierarchical search works on the initial state $|s_1\rangle$ as

$$(58) \quad \mathcal{G}_m \dots \mathcal{G}_3 \mathcal{G}_2 \mathcal{G}_1 |s_1\rangle,$$

where the sub-index denotes position of the GRK in the hierarchy [sequence]. The proof can be written formally in the following way. Define the total number of queries of the hierarchy

$$(59) \quad T(K_1, K_2, \dots, K_m) \equiv S(K_1) + \sum_{i=2}^m \bar{S}(K_{i-1}, K_i).$$

Here K_i is number of "sub"-blocks in the i^{th} partition of database. [We denoted K_1 and K_2 by K and \tilde{K} respectively in previous sections.] $S(K_1)$ is number of queries of the first GRK, and $\bar{S}(K_{i-1}, K_i)$ that of the i^{th} GRK in the hierarchy. Note that S and \bar{S} are not of the same function form. S takes the form corresponding to a direct GRK (25):

$$(60) \quad S(K_1) = \left(\frac{\pi}{4} + \frac{\alpha(K_1) - \eta(K_1)}{\sqrt{K_1}} \right) \sqrt{N}.$$

While \bar{S} takes a form of sequential GRK similar to (45):

$$(61) \quad \bar{S}(K_{i-1}, K_i) = \left(\frac{\pi}{4} - \frac{\alpha(K_{i-1})}{2} + \frac{\alpha(K_i) - \eta(K_i)}{\sqrt{K_i}} \right) \frac{\sqrt{N}}{\sqrt{\prod_{j=1}^{i-1} K_j}}, \quad i \geq 2.$$

[We denoted $S(K_1)$ and $\bar{S}(K_1, K_2)$ by $S(K)$ and $\bar{S}(K, \tilde{K})$ respectively in previous sections.] Let us substitute these expressions into (59):

$$(62) \quad \begin{aligned} & T(K_1, K_2, \dots, K_m) \\ &= \left\{ \frac{\pi}{4} + \sum_{i=1}^{m-1} \frac{\frac{\pi}{4} + \frac{1}{2}\alpha(K_i) - \eta(K_i)}{\sqrt{\prod_{j=1}^i K_j}} + \frac{\alpha(K_m) - \eta(K_m)}{\sqrt{\prod_{i=1}^m K_i}} \right\} \sqrt{N}. \end{aligned}$$

On the other hand, if we partition the database directly into the smallest sub-blocks, then the number of these sub-blocks would be $\prod_{i=1}^m K_i$. A direct GRK will locate the smallest target sub-block. This would require

$$(63) \quad S\left(\prod_{i=1}^m K_i\right) = \left\{ \frac{\pi}{4} + \frac{\alpha(\prod_{i=1}^m K_i) - \eta(\prod_{i=1}^m K_i)}{\sqrt{\prod_{i=1}^m K_i}} \right\} \sqrt{N}$$

queries to the oracle. Therefore the difference of (62) and (63) is

$$\begin{aligned}
 (64) \quad T(K_1, K_2, \dots, K_m) - S\left(\prod_{i=1}^m K_i\right) \\
 = \left\{ \left(\sum_{i=1}^{m-1} \frac{\frac{\pi}{4} + \frac{1}{2}\alpha(K_i) - \eta(K_i)}{\sqrt{\prod_{j=1}^i K_j}} \right) \right. \\
 \left. + \frac{[\alpha(K_m) - \eta(K_m)] - [\alpha(\prod_{i=1}^m K_i) - \eta(\prod_{i=1}^m K_i)]}{\sqrt{\prod_{i=1}^m K_i}} \right\} \sqrt{N}.
 \end{aligned}$$

We will show that this expression is always positive when each $K_i \geq 2$. Using **Lemma 1** (53), we see that each term under the summation of (64) is positive. Using **Lemma 2** (54), $\alpha - \eta$ is a monotonically decreasing function. Note that product of all K_i 's is larger than K_m , we see that the remaining term in the brace of (64) is also positive. Consequently, we conclude our result in the following corollary:

COROLLARY 1.

$$(65) \quad T(K_1, K_2, \dots, K_m) > S\left(\prod_{i=1}^m K_i\right), \quad \forall K_i \in [2, +\infty).$$

i.e. Hierarchy of *arbitrary* number of GRK's makes more queries to the oracle than a direct GRK. *Direct GRK partial search always works faster.*

7. Summary

The present paper studied quantum search. Partial search algorithm is called GRK. We studied partial search hierarchy and compared it with direct partial search [GRK]. Consider database of N items with a single target item [target item also called marked item or solution]. The database is partitioned into K blocks, each block further partitioned into \tilde{K} sub-blocks. Hierarchical search is: use GRK and sequential GRK to find the target block and target sub-block, respectively. Successive GRK's can be made if the database is further partitioned. Each sequential GRK in the hierarchy works faster than the previous one. However, the total number of queries to the oracle adds up. The main conclusion is that *a partial search hierarchy works slower than a direct partial search*, see theorem (56) and corollary (65). For example, consider a database partitioned into 3 blocks. Each block is further partitioned into 3 sub-blocks, so totally there are 9 sub-blocks. One could first find the target block using GRK, then the target sub-block by a sequential GRK. Nevertheless, it is faster to run a GRK partial search directly over the 9 sub-blocks and finds the target sub-block once.

Note: Only the class of algorithms using the standard Grover oracle was considered in the paper. This means that if one has already built the main Grover algorithm experimentally, then we do not need any new hardware to run the GRK algorithm. Another advantage of using the same oracle I_t as the main Grover algorithm is more subtle: We can use ancilla [additional or auxiliary] q-bits to label different partitions of the database into blocks of equal size $b = N/K$. Then we are able to run GRK algorithm simultaneously for different partitions. [See Appendix

D for more details.] Later a user can measure the ancilla q-bits and choose his or her favorite partition, by that time the target block already will be found.

Acknowledgments

The work is supported by NSF Grant DMS-0503712.

Appendix A. Differences of the Last Operation of GRK in Literature

Different versions of the last operation in **Step 3** of GRK appeared in literature. [6, 9, 7] People have finalized [after steps 1 and 2] the state $|v\rangle \equiv G_2^{j_2} G_1^{j_1} |s_1\rangle$ with different operations I_{s_1} , $-I_t I_{s_1}$, or $G_1 \equiv -I_{s_1} I_t$. Grover and Radhakrishnan used I_{s_1} . [6] This makes one less query to the oracle but the amplitude of the target item is negative in the final state $I_{s_1}|v\rangle$. Paper [7] used $-I_t I_{s_1}$ but paper [10] used G_1 . The last two version become the same in the large block limit. This means that final states $-I_t I_{s_1}|v\rangle$ and $G_1|v\rangle$ are equivalent [of the same form] when $b \rightarrow \infty$, though I_{s_1} and I_t do not commute in general. We choose G_1 in our paper because it uses the same Grover iteration.

Appendix B. Ranges of Parameters α and η

We are going to specify ranges of parameters α and η introduced in (21). Because of the constraint (22) relating the two parameters, it is sufficient to specify the range of α . It was shown in [7] that amplitudes [of items in the database after GRK] depend on $\sin(2j_2\theta_2) \sim \sin(2\alpha)$ and $\cos(2j_2\theta_2) \sim \cos(2\alpha)$. So that it is sufficient to take values of α within one period: $\alpha \in [a, a + \pi]$, with a some real number determined later. We are looking for the exact boundaries of α set by physical considerations.

Query numbers (21) are non-negative:

$$(66) \quad j_1 = \left(\frac{\pi}{4} - \frac{\eta}{\sqrt{K}} \right) \sqrt{N} \geq 0,$$

$$(67) \quad j_2 = \frac{\alpha}{\sqrt{K}} \sqrt{N} \geq 0.$$

Total query number (23) should be less than that of a full Grover search:

$$(68) \quad j_1 + j_2 = \left(\frac{\pi}{4} + \frac{\alpha - \eta}{\sqrt{K}} \right) \sqrt{N} \leq \frac{\pi}{4} \sqrt{N}.$$

These three inequalities (66), (67) and (68) yield that

$$(69) \quad 0 \leq \alpha \leq \eta \leq \frac{\pi}{4} \sqrt{K}.$$

We use constraint (22) to express η as a function of α

$$(70) \quad \eta(\alpha) = \frac{1}{2} \sqrt{K} \text{Arctan} \left(\frac{2\sqrt{K} \sin 2\alpha}{K - 4 \sin^2 \alpha} \right)$$

with function $\text{Arctan}(x)$ multi-valued. But according to (69), we have

$$(71) \quad 0 \leq \text{Arctan} \left(\frac{2\sqrt{K} \sin 2\alpha}{K - 4 \sin^2 \alpha} \right) \leq \frac{\pi}{2}.$$

Therefore we could take the principal branch $\arctan(x)$. Now inequality (69) becomes

$$(72) \quad 0 \leq \alpha \leq \frac{1}{2}\sqrt{K} \arctan \left(\frac{2\sqrt{K} \sin 2\alpha}{K - 4 \sin^2 \alpha} \right) \leq \frac{\pi}{4} \sqrt{K}.$$

This inequality determines range of α .

The solution of (69) can be written in the following form:

$$(73) \quad 0 \leq \alpha \leq \alpha_B(K).$$

Here the upper bound $\alpha_B(K)$ is a function of K . When $K = 2, 3$ or 4 , $\alpha_B(K)$ coincide with the singularities of $\eta(\alpha)$. [$K - 4 \sin^2 \alpha = 0$ at these singularities.] When $K \geq 5$, values of $\alpha_B(K)$ can be solved numerically. As K increases, $\alpha_B(K)$ approaches a certain positive number $\alpha_B(\infty)$. This limit $\alpha_B(\infty) = 0.947747\dots$ is the solution of $\alpha = \sin(2\alpha)$. [Inequality $\alpha \leq \eta(\alpha)$ becomes $\alpha \leq \sin(2\alpha)$ as $K \rightarrow \infty$.] The value of $\alpha_B(K)$ always lies in between $\alpha_B(\infty)$ and $\frac{\pi}{2}$ when $K \geq 5$. We list these results in Table B.

Table 2. Upper Bound of α .

K	2	3	4	5	6	100	∞
$\alpha_B(K)$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	1.22683	1.15100	0.956221	0.947747

Appendix C. Minimization of the Total Number of Queries of GRK

Here we give a proof that (24) is the global minimum of $\alpha - \eta$ under constraint (22). In Appendix B we used (22) to express η as a function of α

$$(74) \quad \eta(\alpha) = \frac{\sqrt{K}}{2} \arctan \left(\frac{2\sqrt{K} \sin 2\alpha}{K - 4 \sin^2 \alpha} \right).$$

Now we define a function

$$(75) \quad f(\alpha) \equiv \alpha - \eta(\alpha)$$

which we want to minimize within the range $0 \leq \alpha \leq \alpha_B(K)$. We first prove that (24) is a local minimum of $f(\alpha)$.

C.1. Case $K \geq 3$. The first derivative of $f(\alpha)$ is

$$(76) \quad f'(\alpha) = \frac{16(K-1)\sin^4 \alpha - 4K^2 \sin^2 \alpha + K^2}{16(K-1)\sin^4 \alpha - 8K \sin^2 \alpha - K^2}.$$

It vanishes at (24) with $\sin^2 \alpha = \frac{K}{4(K-1)}$. We calculate next the second derivative

$$(77) \quad f''(\alpha) = \frac{4K \sin 2\alpha [4(K-1)(K-2) \cos^2 2\alpha + 16(K-1) \cos 2\alpha + (K-2)^2(K+2)]}{[16(K-1)\sin^4 \alpha - 8K \sin^2 \alpha - K^2]^2}.$$

Note that the value of the denominator at (24) is $\frac{K^6}{(K-1)^2}$, which is strictly positive as $K \geq 3$. The numerator is also positive because both $\sin 2\alpha$ and $\cos 2\alpha$ are positive at (24) with $K \geq 3$. [See [7] for the range of $\alpha(K)$.] Therefore $f'(\alpha) = 0$ and $f''(\alpha) > 0$ at the solution (24), so that (24) is a local minimum for $K \geq 3$.

C.2. Case $K = 2$. The case that $K = 2$ is more subtle. Expression (24) yields that $\alpha = \frac{\pi}{4}$ and $\eta = \frac{\pi}{2\sqrt{2}}$. However, both first (76) and second (77) derivatives of $\alpha - \eta(\alpha)$ vanish at this critical point. The third derivative is non-zero: $f'''(\alpha = \frac{\pi}{4}) = -4$. So we expand function $\alpha - \eta(\alpha)$ about the critical point

$$(78) \quad \alpha - \eta(\alpha)|_{K=2} = -\frac{4}{3!} \left(\alpha - \frac{\pi}{4} \right)^3 + \mathcal{O} \left(\left(\alpha - \frac{\pi}{4} \right)^4 \right).$$

We see that $\alpha = \frac{\pi}{4}$ is actually a saddle point due to the non-vanishing cubic term. The form (78) suggests that if α goes greater than $\frac{\pi}{4}$, value of function $\alpha - \eta(\alpha)$ could be further reduced than the value at the saddle point. However, $\alpha = \frac{\pi}{4}$ is a boundary set by physical considerations [see Table B]. Definition of α and η in (21) involves query numbers j_1 and j_2 , which are non-negative. Therefore $j_1 \equiv \left(\frac{\pi}{4} - \frac{\eta}{\sqrt{2}} \right) \sqrt{N} \geq 0$, i.e. $\eta \leq \frac{\pi}{2\sqrt{2}}$. Now we allow α to go beyond $\frac{\pi}{4}$ and write

$$(79) \quad \alpha = \frac{\pi}{4} + \delta, \quad \eta = \frac{\pi}{2\sqrt{2}} + \epsilon.$$

Here δ and ϵ are infinitesimals, $\delta > 0$. Then constraint (22) requires that

$$(80) \quad \epsilon = \delta.$$

So that η would be greater than the physically allowed maximal value $\frac{\pi}{2\sqrt{2}}$ and j_1 would be negative $j_1 = -\frac{\delta}{\sqrt{2}}\sqrt{N}$. This analysis showed that α can never go beyond $\frac{\pi}{4}$ and function $\alpha - \eta(\alpha)$ is minimized at this boundary. Therefore, expression (24) as a local minimum is also valid in the case that $K = 2$.

Now we have proved that the critical point (24)

$$(81) \quad \alpha(K) = \frac{1}{2} \arccos \left(\frac{K-2}{2(K-1)} \right)$$

is a local minimum of $f(\alpha)$. Note that $f(\alpha)$ is analytical as $0 \leq \alpha \leq \alpha_B(K)$ and there is no singularity in this range any more. Therefore we can show that this local minimum (81) is also global by comparing the value of $f(\alpha)$ at (81) with those at the boundaries. [We always have $0 < \alpha(K) \leq \alpha_B(K)$ and equality holds only for $K = 2$.] We list the comparison results for $K = 2, 3$ and 4 in Table C.2.

Table 3. Comparison of values of $f(\alpha)$ at different points.

K	$f(0)$	$f(\alpha(K))$	$f(\alpha_B(K))$
2	0	$\frac{\pi}{4} (1 - \sqrt{2}) \approx -0.325323$	$\frac{\pi}{4} (1 - \sqrt{2}) \approx -0.325323$
3	0	-0.337098	-0.313152
4	0	-0.339837	0

When $K \geq 5$, $f(0) = f(\alpha_B(K)) = 0$, while $f(\alpha(K)) < 0$. Therefore, we conclude that the critical point (24) or (81) is always the global minimum.

Appendix D. Different Partitions of a Database

A data base of N items can be partitioned into blocks in different ways. For example, items in one block may have the first 3 bits of their addresses the same

for one partition or the last 3 bits the same for another partition. For a database partitioned into K blocks of equal size $b = N/K$, there are totally

$$(82) \quad P(N, K) = \frac{N!}{(b!)^K K!}$$

different ways of partition. We could use ancilla q-bits [also called additional or auxiliary q-bits] to label these partitions. As N and b both being large, we shall need

$$(83) \quad \log_2 P(N, K) \sim N \log_2 K - \log_2 K!$$

ancilla q-bits. For example, if we have $N = 4$ items and $K = 2$ blocks, then the number of partitions is $P(4, 2) = 3$ and we shall need $\log_2 3 \approx 2$ ancillas. In practice, The number (83) can be further reduced if we only label the partitions commonly used, not all partitions. Then we can run GRK simultaneously for those selected partitions. When a user measures ancilla q-bit in his/her favorite partition, the target block will already be found by that time.

References

- [1] T. H. Cormen, C. E. Leiserson, R. E. Leiserson, R. L. Rivest and C. Stein, *Introduction to Algorithms* (MIT Press, 2003), 2nd ed.
- [2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
- [3] R. Cleve, A. Ekert, L. Henderson, C. Macchiavello and M. Mosca, *Complexity* **4**, 33 (1998), quant-ph/9903061.
- [4] L. K. Grover, Proceedings, *28th Annual ACM Symposium on the Theory of Computing (STOC)* (1996), 212, quant-ph/9605043.
- [5] M. Heiligman, quant-ph/0006136.
- [6] L. K. Grover and J. Radhakrishnan, *ACM Symp. on Parallel Algorithms and Architectures, Las Vegas, Nevada, USA* (2005), 186, quant-ph/0407122.
- [7] V. E. Korepin, *J. of Phys. A* **38**, L731 (2005), quant-ph/0503238.
- [8] V. E. Korepin and J. Liao, *Quantum Information Processing* **5**, 209 (2006), quant-ph/0510179.
- [9] B.-S. Choi and V. E. Korepin, *Quantum Information Processing* **6**, 97 (2007), quant-ph/0608106.
- [10] V. E. Korepin and B. C. Vallilo, *Prog. Theor. Phys.* **116**, 783 (2006), quant-ph/0609205.
- [11] M. Mosca, *Theoretical Computer Science* **264**, 139 (2001).
- [12] V. E. Korepin and L. K. Grover, *Quantum Information Processing* **5**, 5 (2006), quant-ph/0504157.

C.N. YANG INSTITUTE FOR THEORETICAL PHYSICS, STATE UNIVERSITY OF NEW YORK AT STONY BROOK, STONY BROOK, NY 11794-3840, USA

E-mail address: korepin@max2.physics.sunysb.edu

DEPARTMENT OF PHYSICS AND ASTRONOMY, STATE UNIVERSITY OF NEW YORK AT STONY BROOK, STONY BROOK, NY 11794-3800, USA

E-mail address: yixu@ic.sunysb.edu

This volume represents the talks given at the Conference on Interactions between Representation Theory, Quantum Field Theory, Category Theory, Mathematical Physics, and Quantum Information Theory, held in September 2007 at the University of Texas at Tyler.

The papers in this volume, written by top experts in the field, address physical aspects, mathematical aspects, and foundational issues of quantum computation.

This volume will benefit researchers interested in advances in quantum computation and communication, as well as graduate students who wish to enter the field of quantum computation.

ISBN 978-0-8218-4627-8



CONM/482

AMS on the Web
www.ams.org