CONTEMPORARY MATHEMATICS

536

Cross Disciplinary Advances in Quantum Computing

NSF Sponsored Research Conference on
Representation Theory, Quantum Field Theory,
Category Theory, and Quantum Information Theory
October 1–4, 2009
University of Texas at Tyler
Tyler, Texas

Kazem Mahdavi
Deborah Koslover
Leonard L. Brown III
Editors

American Mathematical Society

CONTEMPORARY MATHEMATICS

536

Cross Disciplinary Advances in Quantum Computing

NSF Sponsored Research Conference on
Representation Theory, Quantum Field Theory,
Category Theory, and Quantum Information Theory
October 1–4, 2009
University of Texas at Tyler
Tyler, Texas

Kazem Mahdavi
Deborah Koslover
Leonard L. Brown III
Editors

American Mathematical Society
Providence, Rhode Island

2000 *Mathematics Subject Classification.* Primary 81P68, 81–01, 81–02, 81–06.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Library of Congress Cataloging-in-Publication Data

Conference on Representation Theory (2009 : University of Texas at Tyler)

Cross disciplinary advances in quantum computing : Conference on Representation Theory, Quantum Field Theory, Category Theory, and Quantum Information Theory, October 1–4, 2009, University of Texas at Tyler, Tyler, Texas / Kazem Mahdavi, Deborah Koslover, Leonard L. Brown, III, editors.

p. cm. — (Contemporary mathematics ; v. 536)

Includes bibliographical references.

ISBN 978-0-8218-4975-0 (alk. paper)

1. Quantum theory—Mathematics—Congresses. 2. Quantum communication—Congresses. I. Mahdavi, Kazem. II. Koslover, Deborah. III. Brown, Leonard L., 1972– IV. Title.

QC174.17.M35C66 2009

530.12—dc22

2010045181

Contents

This page intentionally left blank

Preface

Building on the success of the 2007 conference, the 2009 Conference on Representation Theory, Quantum Field Theory, Category Theory, and Quantum Information Theory, was held October 1–4 at the University of Texas at Tyler. It 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, Air Force Office of Scientific Research, Los Alamos and Argonne National Lab; and major education institutions including Harvard, Oxford, and Moscow State University.

Our main purpose in publishing this proceedings volume 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 seven 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.

As a general rule, every book is written with the goal of expanding the horizon of human knowledge. 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 wonderful speakers: Samson Abramsky (Oxford), Paul Benioff (Argonne), Robert Bonneau (AFOSF), Howard Brandt (ARL), Sergey Bravyi (IBM), Bob Coecke (Oxford), Denis Ilyutko (Moscow), Louis Kauffman (Illinois), Vladimir Korepin (Stony Brook), Sam Lomonaco (Maryland), John Myers (Harvard), David Radford (Illinois) and Yong Shi Wu (Utah).

Next we would like to thank the University of Texas at Tyler for hosting the event.

Finally, the editors would like to thank the NSF for funding the conference (DMS 0901385).

Kazem Mahdavi
Deborah Koslover
Leonard L. Brown, III

This page intentionally left blank

List of Participants

Samson Abramsky
Oxford University Computing Laboratory

Paul Benioff
Argonne National Laboratory

Robert Bonneau
Air Force Office of Scientific Research

Howard Brandt
Army Research Laboratory

Sergey Bravyi
IBM Research

Leonard L. Brown, III
University of Texas at Tyler

Goong Chen
Texas A&M University

Bob Coecke
Oxford University Computing Laboratory

Heather Dye
McKendree University

Denis Ilyutko
Moscow State University

Louis Kauffman
University of Illinois at Chicago

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

David Radford
University of Illinois at Chicago

Eric Rowell
Texas A&M University

Yong Shi Wu
University of Utah

This page intentionally left blank

Contemporary Mathematics
Volume **536**, 2011

Cartan Decomposition and Entangling Power of Braiding Quantum Gates

A. D. Ballard and Yong-Shi Wu

Abstract. In this paper we report our recent progress in quantifying the entangling power of two-qubit and three-qubit quantum gates. By using the Cartan decomposition technique for multi-qubits, we have successfully extended existing formalism for the entangling power from the case of two-qubit gates to that of three-qubit gates, for the entanglement between one fixed qubit and the other two as a second subsystem. Particular attention is paid to the quantum gates which implement topological braiding operations, such as the Kauffman-Lomonaco two-qubit gate that produces the Bell states from the computational basis, and the three-qubit gate that produces the GHZ states from the computational basis. We find that the Kauffman-Lomonaco gate has a maximal entangling power, while the GHZ gate does not. We also note that the three-qubit gate that produces the Werner states, though not a braiding gate, has a maximal entangling power.

1. Introduction

Entanglement, as non-classical and non-local correlation peculiar to the quantum world, is known to be an important resource for quantum information processing and quantum computing. It has been shown to be crucial for algorithms such as teleportation and quantum key distribution and for solving problems that are exponentially difficult in classical computation. So more and deeper understanding of how to produce and quantify quantum entanglement remains one of the central problems in the field of quantum information. In this paper we report our recent progress in quantifying the entangling power of two-qubit and three-qubit *braiding* quantum gates that have been proposed recently.

A recent approach to understanding quantum entanglement is motivated by an analogy [**1**] between entangled quantum states and topological entanglement known in knots. In ref. [**2**], Kauffman and Lomonaco introduced two-qubit braiding quantum gates, which carry out braiding operations of qubits, in a way similar to those in the theory of knots and links. They have shown that the two-qubit braiding gates are universal, when used together with one-qubit gates. In principle, quantum circuits consisting of only braiding gates may be used to implement the so-called *topological quantum computation* [**3, 4, 5**], a new approach to implementing

1991 *Mathematics Subject Classification.* Primary 81-06, 94-06.
Key words and phrases. quantum information, lie algebra, representation theory.

fault-tolerant quantum computation. Another advantage of the two-qubit braiding gate proposed by Kauffman and Lomonaco is that it produces the well-known (maximally entangled) Bell states when acting upon computational basis states, which are non-entangled. More recently, a three-qubit braiding quantum gate has been proposed in refs. [**6, 7, 8**]. It has been shown that this gate, when acting upon the computational basis, produces the famous (entangled three-qubit) GHZ states. Therefore, in consistency with the analogy with topological entanglement in knots and links, braiding gates indeed produce quantum entanglement among the qubits in a quantum circuit.

For the benefit of efficiently producing entanglement, one important question about the braiding gates is how to quantify their entangling power. Conceptually the entangling power of a quantum gate (or an operator) refers to its ability to produce entanglement between the qubits they act on or, more precisely, its ability to produce entangled states from product states (or computational basis states). To quantify entangling power and operator entanglement, we need to employ some of the tools for quantifying state entanglement, and use an isomorphic map from the operator space to the state space. Along this line of thought, several authors have developed formal methods to quantify the entangling power of operators acting on two qubits, which form the Lie group SU(4) [**19, 15, 22, 23, 21, 14, 24**]. In particular, it has been shown that one can quantify the entangling power of any SU(4) operator by introducing the so-called magic matrix [**14, 24, 23**], which contains much fewer parameters, but does not lose any genuine two-qubit entanglement. Physically this is easy to understand, since the entangling power for genuine two-qubit entanglement is known to be unchanged under any one-qubit operation of either qubit, which form an $SU(2)\otimes SU(2)$ subgroup of $SU(4)$. Mathematically, an arbitrary $SU(4)$ operator can be represented by a representative magic matrix through a Cartan decomposition of the symmetric space $SU(4)/SU(2)\otimes SU(2)$ [**12**], if we do not care about local one-qubit operations.

In the course of studying the entangling power of three-qubit braiding gates, it was natural for us to generalize the above magic-matrix technique to three-qubit operators, which now form the Lie group $SU(8)$. The entangling power we want to compute is that for a bipartite three-qubit system. (Right now entangling power is defined only for a bipartite system; see, e.g., refs. [**20, 19**].) The three-qubit braiding gates proposed in [**6**] can actually be understood as the braiding between the first qubit and the other two as a whole [**7**]. The entangling power of such three-qubit braiding gates is invariant under the local operations of $SU(2)\otimes SU(4)$. But $SU(8)/SU(2)\otimes SU(4)$ is *not* a symmetric space as in the two-qubit case. Therefore, we need to adopt a recursive Cartan decomposition technique [**13**] to define the three-qubit magic matrix, and construct it for three-qubit braiding gates that we are interested in. In this way, we have been able to compute the (bipartite) entangling power of three-qubit gates, especially those of braiding gates. Since our work is the first step going beyond two-qubit entangling power, we expect that our method may be useful in further study of multi-qubit entanglement, such as entanglement combing[**17**], as well as that of the discord and entanglement for mixed states [**9, 10**].

Our paper is organized as follows. In Sec. 2, we give a brief review of the braiding quantum gates, and of bipartite entangling power. Here we recall that the entanglement measure used in defining entangling power is the linear entropy (see,

e.g., [**19**]), because it is easy to compute. In Sec. 3 and 4, we first review the magic matrix method for a two-qubit gate, and then use it to show that various two-qubit braiding gates have the maximal entangling power. In Sec. 5, we extend the theory of entangling power to a three-qubit gate. In Sec. 6, we present a recursive Cartan decomposition to introduce the magic matrix for the (bipartite) entangling power between the first and the remaining two qubits for a three-qubit gate. In Sec. 7, we use the results of Sec. 5 and 6 to compute the entangling power of the GHZ generators as three-qubit braiding gates and of some non-braiding gates.

We note that the three-qubit case is more complicated than the two-qubit case, because $SU(4)/SU(2)\otimes SU(2)$ is a symmetric space, while $SU(8)/SU(2)\otimes SU(4)$ is *not*. So we need to use a recursive Cartan decomposition [**13**] of $SU(8)$, and an additional non-commuting entangling operator appears in the composition. Our results indicate that for the (bipartite) entangling power, the GHZ generators are not maximal, while the generators of the entangled Werner states are.

2. Brief review of braiding gates and entangling power

2.1. Braiding quantum gates. A two-qubit braiding quantum gate is an $\check{R}$-matrix (with $p=2$) satisfying the braided Yang-Baxter equations (YBE) [**2**]:

$$(\check{R}\otimes \mathbb{1}_p)(\mathbb{1}_p\otimes \check{R})(\check{R}\otimes \mathbb{1}_p)=(\mathbb{1}_p\otimes \check{R})(\check{R}\otimes \mathbb{1}_p)(\mathbb{1}_p\otimes \check{R}). \tag{1}$$

Here the $p^2\times p^2$ matrix $\check{R}$: $V\otimes V\to V\otimes V$, where $V=\mathbb{C}^p$, is unitary. The relation (1) gives rise to a sequence of representations $(\pi_n,(\mathbb{C}^p)^{\otimes n})$ of the braid group $\mathcal{B}_n$: $\pi_n(b_i)=\mathbb{1}_p^{\otimes i-1}\otimes\check{R}\otimes\mathbb{1}_p^{\otimes n-i-1}$, since clearly $\pi_n(b_i)$ satisfy the braid group relations.

A three-qubit braiding quantum gate is a special case of the following definition for solutions of the generalized Yang-Baxter equation [**7, 6**]:

Definition Fix p with $2\le p\in\mathbb{N}$ and let $l=p^k$. A unitary $p^N\times p^N$ matrix $\check{R}$ is a solution to the *generalized* Yang-Baxter equations, if

$$(\check{R}\otimes \mathbb{1}_l)(\mathbb{1}_l\otimes \check{R})(\check{R}\otimes \mathbb{1}_l)=(\mathbb{1}_l\otimes \check{R})(\check{R}\otimes \mathbb{1}_l)(\mathbb{1}_l\otimes \check{R}), \tag{2}$$

as operators on $(\mathbb{C}^p)^{\otimes(k+N)}$.

When $N=2,k=1$, the generalized YBE (2) is the same as the conventional YBE (1). If $k\ge N/2$, the assignment $\pi_n(b_i)=\mathbb{1}_l^{\otimes i-1}\otimes\check{R}\otimes\mathbb{1}_l^{\otimes n-i-1}$ defines a sequence of representations $(\pi_n,(\mathbb{C}^p)^{\otimes(N+k(n-2))})$ of the braid group $\mathcal{B}_n$. The special case with $p=2,N=3,k=2$ gives rise to a three-qubit braiding gate, with braiding between the first qubit and the other two.

For examples of two- and three-qubit braiding gates, see the references [**2, 6, 7**], and Sec. 4 and 7 in this paper.

2.2. Entanglement and Entangling power. We consider the entangling power of an operator of a bipartite system, with Hilbert spaces, $\mathcal{H}_1$ and $\mathcal{H}_2$, for subsystems labelled 1 and 2, respectively. The quantity we use to quantify entanglement in a state (with density operator ρ) of the total system is the linear entropy, $E(\rho)=1-tr_1(\rho_1^2)$, where $\rho_1=tr_2(\rho)$ is the reduced density operator of subsystem 1, and tr_1 and tr_2 the partial trace over subsystems 1 and 2, respectively. The linear entropy can be viewed as a linearized version of the von Neumann entanglement entropy. For a product state, $E(\rho)=0$, so the linear entropy measures the impurity of the subsystem, thus indirectly the entanglement of the composite system. One uses the linear entropy in defining entangling power, because it is easy to compute.

The idea for defining the entangling power of an operator (or quantum gate) is to lift the notion of entanglement from the state level to the operator level [**19**]. For an operator U acting on $\mathcal{H}_{total} = \mathcal{H}_1 \otimes \mathcal{H}_3$, it is known that it belongs to the Hilbert-Schmidt space $\mathcal{H}_{HS,total}$, which is isomorphic, as a Hilbert space, to $\mathcal{H}_{total}^{\otimes 2}$. The natural isomorphism, Ψ, from the operator to the state space is known to be

$$\big|\Psi(U)\big\rangle := (U \otimes \mathbb{1})\big|\Phi^+\big\rangle, \tag{3}$$

with the ket, $\big|\Phi^+\big\rangle := \sum_{\alpha=1}^{d_1 d_3} \big|\alpha\big\rangle^{\otimes 2}$, and $\{\big|\alpha\big\rangle\}$ $(\alpha = 1, \cdots, d_1 d_3)$ forming an orthonormal basis of $\mathcal{H}_{total}$. With this map, the entanglement of operator U is defined [**19**] as the linear entropy of the state $\big|\Psi(U)\big\rangle$; i.e. $E(U) := E(\Psi(U))$.

For a bipartite system with Hilbert space $\mathcal{H}^{\otimes 2}$, an operator U lives in $\mathcal{H}_{HS,total}^{\otimes 2}$ $\cong \mathcal{H}^{\otimes 4}$, and the map Ψ is given by

$$\big|\Psi(U)\big\rangle := (U_{13} \otimes \mathbb{1}_{24})\big|\Phi^+\big\rangle, \tag{4}$$

with the subscripts of U indicating on which $\mathcal{H}$ the operator acts. (Our notation here is slightly different from that in ref. [**19**].) For two qubits, the single-qubit Hilbert space $\mathcal{H}$ is two-dimensional; the subscripts of U indicate on which qubits the operator acts.

With this map, we can measure the entanglement of a unitary operator U with the linear entropy of the mapped state $\big|\Psi(U)\big\rangle$. On the other hand, we define the entangling power of an operator, U, as the averaged entanglement produced by it over all product states $\big|\psi\big\rangle \otimes \big|\phi\big\rangle$ distributed according to a certain probability density $p(\psi, \phi)$ over the manifold of product states:

$$e_p(U) := \overline{E(U\big|\psi\big\rangle \otimes \big|\phi\big\rangle)}^{p(\psi,\phi)}. \tag{5}$$

A natural choice for the probability density distribution $p(\psi, \phi)$ over the manifold of product states is the uniform distribution, which is a $U(2) \otimes U(2)$-invariant probability distribution, i.e., $p(\psi_1, \psi_3) = p(U_1\psi_1, U_3\psi_3)$. From the above definition with the uniform distribution, it was shown [**19**] that the entangling power of U is related to the entanglement $E(U)$, given by the linear entropy, and the swap between the first and third qubits by the following relation:

$$e_p(U) = E(U) + E(US) - E(S). \tag{6}$$

The entangling power quantifies the ability of an operator to produce entangled states from a uniform product state, which can be maximally entangled [**18**]. It is invariant under local unitary operations, that is, operators that can be written as $U_1 \otimes U_3$, do not change the entangling power [**20**]. Thus any operator in the local equivalence class of the identity and swap has zero entangling power. In the case of the swap, we have an example of an operator that is non-local, but nevertheless has zero entangling power.

While this formula is convenient, we can do better. It is useful to introduce the magic matrix.

3. Magic matrix and Cartan decomposition of $SU(4)$

The idea behind the magic matrix proposed in Refs. [**13, 15, 14**] is the following: Since entangling power is invariant under local unitary rotations of each subsystem, we want to extract the completely non-local entangling operation of any

operator, apart from local rotations of either subsystem. The magic matrix represents such a completely non-local entangling operation hidden in any operator. Mathematically it is required that any unitary operators of the total system are related to a magic matrix by local unitary operations, which act only on one of the subsystems. Thus the computation of the entangling power of any operator of the total system is reduced to the computation of that of the magic matrix associated with it.

For simplicity, let us consider a two-qubit system. There exists a mathematical theorem (see below) stating that all two-qubit unitary operators in $SU(4)$ are related to a magic matrix by local unitary operations in $SU2)\otimes SU(2)$. Thus, the computation of the entangling power of any operator in $SU(4)$ is reduced to the computation of that of the magic matrix associated with it in the coset space $SU(4)/SU(2)\otimes SU(2)$, which is known to be a symmetric space [**12**]. Actually the magic matrix does not need to run over the whole symmetric space. The magic matrix can be generated by exponentiation of a maximal abelian subalgebra (called the Cartan subalgebra) associated with the symmetric space [**13**]. Mathematically this procedure corresponds to the Cartan decomposition of $SU(4)$ associated with the Lie algebra pair $(\mathfrak{su}(4),\mathfrak{su}(2)\oplus\mathfrak{su}(2))$ [**13**]. More concretely, we have [**13, 15**]

Theorem $G\equiv SU(4)$ has the following (Cartan) decomposition $G=KMK$, where $K\equiv SU(2)\otimes SU(2)$ and

$$M=e^{-i(c_1\sigma_x\otimes\sigma_x+c_2\sigma_y\otimes\sigma_y+c_3\sigma_z\otimes\sigma_z)}. \tag{7}$$

In the computational basis, this magic matrix is explicitly given by

$$U_d=\begin{pmatrix} e^{-ic_3}c^- & 0 & 0 & -ie^{-ic_3}s^- \\ 0 & e^{ic_3}c^+ & -ie^{ic_3}s^+ & 0 \\ 0 & -ie^{ic_3}s^+ & e^{ic_3}c^+ & 0 \\ -ie^{-ic_3}s^- & 0 & 0 & e^{-ic_3}c^-. \end{pmatrix}$$

with $c^\pm=\cos(c_1\pm c_2), s^\pm=\sin(c_1\pm c_2)$. The matrix U_d has the magic basis as eigenvectors, so is diagonal in that basis. In the two-qubit case, the magic basis vectors are nothing but the Bell states:

$$\big|\Phi_1\big\rangle=\frac{1}{\sqrt{2}}(\big|00\big\rangle+\big|11\big\rangle),\quad \big|\Phi_2\big\rangle=\tfrac{-i}{\sqrt{2}}(\big|00\big\rangle-\big|11\big\rangle)$$
$$\big|\Phi_3\big\rangle=\frac{1}{\sqrt{2}}(\big|01\big\rangle-\big|10\big\rangle),\quad \big|\Phi_4\big\rangle=\tfrac{-i}{\sqrt{2}}(\big|01\big\rangle+\big|10\big\rangle).$$

A proof is given in [**14**] in terms of linear transformations.

However, later in this paper when we want to generalize the magic matrix method to the three-qubit case, we need to employ the whole machinery developed in [**13**]. So here in the following we present a proof of the above theorem in terms of the orthogonal Lie algebra pair and the Cartan decomposition.

Definition Let $\mathfrak{g}$ be a real semi-simple Lie algebra and let the decomposition $\mathfrak{g}=\mathfrak{m}\oplus\mathfrak{l}$, $\mathfrak{m}=\mathfrak{l}^\perp$, satisfy the following commutation relations:

$$[\mathfrak{l},\mathfrak{l}]\subset\mathfrak{l},\ [\mathfrak{m},\mathfrak{l}]=\mathfrak{m},\ [\mathfrak{m},\mathfrak{m}]\subset\mathfrak{l}. \tag{8}$$

We refer to this decomposition as a Cartan decomposition of $\mathfrak{g}$.

Definition If $\mathfrak{h}$ is a subalgebra of $\mathfrak{g}$ contained in $\mathfrak{m}$, then $\mathfrak{h}$ is abelian because $[\mathfrak{m},\mathfrak{m}]\subset\mathfrak{l}$. A *maximal* abelian subalgebra contained in $\mathfrak{m}$ is called a Cartan subalgebra of the pair $(\mathfrak{g},\mathfrak{l})$.

The two-qubit magic matrix is a well known result for the case with $\mathfrak{g} = \mathfrak{su}(4)$. It has the direct sum decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{l}$, where

$$\begin{aligned} \mathfrak{l} &= span\ i\{\sigma_x \otimes \mathbb{1}, \sigma_y \otimes \mathbb{1}, \sigma_z \otimes \mathbb{1}, \\ &\quad \mathbb{1} \otimes \sigma_x, \mathbb{1} \otimes \sigma_y, \mathbb{1} \otimes \sigma_z\}, \\ \mathfrak{m} &= span\ i\{\sigma_x \otimes \sigma_x, \sigma_x \otimes \sigma_y, \sigma_x \otimes \sigma_z \\ &\quad \sigma_y \otimes \sigma_x, \sigma_y \otimes \sigma_y, \sigma_y \otimes \sigma_z \\ &\quad \sigma_z \otimes \sigma_x, \sigma_z \otimes \sigma_y, \sigma_z \otimes \sigma_z\} \end{aligned}$$

are vector spaces spanned with real coefficients and satisfying the commutation relations (8). The subalgebra $\mathfrak{l} = \mathfrak{su}(2) \oplus \mathfrak{su}(2)$, generates the subgroup, $K = SU(2) \otimes SU(2)$, which are the local unitary operations.

Furthermore,

$$\mathfrak{h} = span\ i\{\sigma_x \otimes \sigma_x, \sigma_y \otimes \sigma_y, \sigma_z \otimes \sigma_z\} \tag{9}$$

is contained in $\mathfrak{m}$ and is maximal abelian and hence a Cartan subalgebra of the symmetric space $\exp(\mathfrak{m}) = SU(4)/SU(2) \otimes SU(2)$. We define the magic matrix $M = \exp(\mathfrak{h})$ using this Cartan subalgebra, which leads to Eq. (7). The above theorem in differential geometry [**12, 13**] asserts that the Lie group $G = SU(4)$ has a Cartan decomposition $G = KMK$, because the symmetric-space conditions (8) are satisfied. Thus, any $SU(4)$ operator can be related to a magic matrix with merely local operations.

4. Entangling power of two-qubit braiding gates

We first present the general formula for entangling power of an arbitrary two-qubit gate, and then we apply it to various two-qubit braiding gates.

4.1. General entangling power formula. One can easily calculate the entangling power of the magic matrix (7), which contains three parameters, by starting from Eq. (6), and thus obtain [**15**]

$$e_p(M) = \frac{1}{9}[3 - (\cos 4c_1 \cos 4c_2 + \cos 4c_2 \cos 4c_3 + \cos 4c_3 \cos 4c_1)]. \tag{10}$$

For any two-qubit operator in $SU(4)$, one needs to find its Cartan decomposition, and extract the associated magic matrix, thus determining the value of the constants c_1, c_2, and c_3 in Eq. (7). Substituting these constants in Eq. (10), one determines the entangling power.

Alternatively, because the local unitary transformation does not change the determinant (in particular the characteristic equation) we may also determine the constants by directly comparing the eigenvalues of the magic matrix with the eigenvalues of the operator in question, up to a global phase. Below, we show this calculation for some braiding operators.

It is easy to show that the maximum entangling power for a two-qubit operator corresponds to $\{c_1, c_2, c_3\} = \{\pi/4, \phi, 0\}$ (and its permutations, but we may always set their ordering as given above), with $0 \leq \phi \leq \pi/4$, $\pi/2$ periodic around $\pi/4$ (see, e.g., [**15, 14**]). We also see that for this range of constants, $e_p(M) = 4/9$.

4.2. Entangling power of braiding operators. First we compute the entangling power for a six-vertex braiding operator directly from its definition. Then we use the magic matrix method for some other braiding operators.

4.2.1. *Braiding operator, six-vertex.* As an example, we consider a six-vertex braiding operator b, and its composition with the swap S:

$$b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \; bS = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Starting with the uniform state,

$$\big|\Phi^+\big\rangle = \frac{1}{2}\sum_{i,j=0}^{d-1} \big|ii\big\rangle_{12} \otimes \big|jj\big\rangle_{34}, \tag{11}$$

the map (3) or (4) is now given by

$$\big|\Psi(b)\big\rangle = \frac{1}{2}\sum_{i,j=0}^{d-1} (b_{13} \otimes \mathbb{1}_{24})\big|ii\big\rangle_{12} \otimes \big|jj\big\rangle_{34}, \tag{12}$$

Then with

$$Tr\rho_b^2 = \frac{1}{4}, \; Tr\rho_{bS}^2 = \frac{1}{2}$$

we get the entangling power (with $d = 2$)

$$e_p(b) = \frac{d^4 + d^2 - d^4[Tr\rho_{bS}^2 + Tr\rho_b^2]}{d(d-1)(d+1)^2} = \frac{4}{9}.$$

Here ρ_b and ρ_{bS} are the reduced density operators for qubits 1 and 2, which are the qubits owned by, say, Alice. The value 4/9 achieves the maximal entangling power for a two-qubit gate.

4.2.2. *More braiding operators.* The examples of braid group operators we consider here are those apprearing in ref. [**26**]:

$$b_6 = \frac{i}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; b_I = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix},$$

$$b_{IV} = \frac{1-i}{2}\begin{pmatrix} i & 0 & 0 & 1 \\ 0 & 1 & i & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{pmatrix}.$$

We can determine their entangling power by finding the unitary transformation to the magic matrix and determining the constants, c_1, c_2, and c_3. For the Bell matrix (braiding operator b_I), the constants are $c_1 = 0$, $c_2 = \pi/4$, and $c_3 = 0$. The eigenvalues of b_I are $\lambda_1 = 1 + i$ and $\lambda_2 = 1 - i$, which are the same for the magic matrix with the same choice of constants. Further results are given in the table 1.

This same transformation matrix transforms the Bell eigenstates,

$$\big|\Phi_1\big\rangle = \frac{1}{\sqrt{2}}(\big|00\big\rangle + i\big|11\big\rangle), \quad \big|\Phi_2\big\rangle = \tfrac{1}{\sqrt{2}}(-i\big|00\big\rangle - \big|11\big\rangle)$$

$$\big|\Phi_3\big\rangle = \frac{1}{\sqrt{2}}(\big|01\big\rangle - i\big|10\big\rangle), \quad \big|\Phi_4\big\rangle = \tfrac{1}{\sqrt{2}}(i\big|01\big\rangle - \big|10\big\rangle),$$

to the magic matrix eigenstates.

TABLE 1. **Magic matrix parameters for two-qubit braiding operators, B gates, and three-qubit GHZ and Werner operators.** $\{c_1, c_2, c_3\} = \{\pi/4, \phi, 0\}, 0 \leq \phi \leq \pi/4$ gives the domain of maximal entangling power for SU(4), with $\pi/2$-periodicity, and $\{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8\} = \{\pi/4, \pi/4, 0, \phi, 0, 0, 0, 0\}$ is a maximal choice for SU(8). The B gates have been shown to be the most efficient for constructing arbitrary two-qubit unitary operators [**15, 27**]. The last four are three-qubit gates (see below Sec. 7).

OPERATOR	EIGENVALUES	$\{c_i\}$
b_6	1, i, -i	$\{\frac{\pi}{4}, \frac{\pi}{4}, 0\}$
b_I	1+i, 1-i	$\{\frac{\pi}{4}, 0, 0\}$
b_{IV}	1+i, 1-i, -1+i	$\{\frac{\pi}{4}, \frac{\pi}{4}, 0\}$
B	$e^{\pm\frac{\pi}{8}}$, $e^{\pm\frac{3\pi}{8}}$	$\{\frac{\pi}{4}, \frac{\pi}{8}, 0\}$
$B_{8,1}$	1+i, 1-i	$\{\frac{\pi}{4}, 0, 0, 0, 0, 0, 0, 0\}$
$B_{8,2}$	1+i, 1-i	$\{\frac{\pi}{4}, 0, 0, 0, 0, 0, 0, 0\}$
$B_{8,3}$	1+i, 1-i	$\{\frac{\pi}{4}, 0, 0, 0, 0, 0, 0, 0\}$
$\mathcal{W}$	1, i, -i	$\{\frac{\pi}{4}, \frac{\pi}{4}, 0, \phi, 0, 0, 0, 0\}$

5. Entangling power for three-qubit gates

The explicit formulas for entangling power of two-qubit gates were given by Zanardi and collaborators in Refs. [**20, 19**]. To examine the three-qubit braiding gates, we need to generalize the existing formulas. Obviously the bipartite split of three qubits can not be balanced. We assume the bipartition is between the first and the remaining two qubits.

For an arbitrary bipartite split with $\mathcal{H}_1 \otimes \mathcal{H}_3$, operators live in $\mathcal{H}_1^{\otimes 2} \otimes \mathcal{H}_3^{\otimes 2}$. With $d_1 = dim(\mathcal{H}_1)$ and $d_3 = dim(\mathcal{H}_3)$, then $\big|\Phi^+\big\rangle := \sum_{\beta=1}^{d_1}\sum_{\gamma=1}^{d_3}\big|\beta\big\rangle^{\otimes 2}\big|\gamma\big\rangle^{\otimes 2}$, and the map (4) is of a similar form

$$\big|\Psi(U)\big\rangle := (U_{13} \otimes \mathbb{1}_{24})\big|\Phi^+\big\rangle,$$

with U acting on $\mathcal{H}_1 \otimes \mathcal{H}_3$.

Now we can quantify the entanglement of unitary operators across the bipartite split by the linear entropy of the mapped state $\big|\Psi(U)\big\rangle$. Then we define the entangling power of an operator, U, as the averaged entanglement produced by it over all product states with a uniform distribution over the manifold of product states,

$$e_p(U) := \overline{E(U\big|\psi\big\rangle \otimes \big|\phi\big\rangle)}^{p(\psi,\phi)}. \tag{13}$$

where p is the uniform probability density distribution over the manifold of product states, which is a $U(d_1) \otimes U(d_3)$-invariant probability distribution, i.e., $p(\psi_1, \psi_3) = p(U_1\psi_1, U_3\psi_3)$.

As for the relation (6) between the entangling power of U and its operator entanglement, unfortunately, it was derived for the two-qubit case. Fortunately, we have managed to show that a formula of the same form can be derived for the three-qubit case. But we must use a new swap operator that acts across the bipartite

split given by

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{14}$$

In the two-qubit case, we require $(S\otimes S)\, T_{24}\, (S\otimes S) = T_{13}$, where $S\otimes S = S_{12}\otimes S_{34}$. With the new swap, this holds only under the trace. Loosely following the notation in [**19**], with $\langle A, B\rangle := tr(A^\dagger B)$ the Hilbert-Schmidt inner product, the key step is to show that the following still holds:

$$\begin{aligned} & \langle U^{\otimes 2} T_{24} U^{\dagger\otimes 2}, T_{13}\rangle \\ = \; & \langle U^{\otimes 2} S_{12}^2 \otimes S_{34}^2 T_{24} S_{12}^2 \otimes S_{34}^2 U^{\dagger\otimes 2}, T_{13}\rangle \\ = \; & \langle (US)^{\otimes 2} T_{13} (US)^{\dagger\otimes 2}, T_{13}\rangle \\ = \; & d_1^2 d_2^2 [1 - E(US)]. \end{aligned}$$

In summary, Eq. (6) with the new swap operator is shown to be valid, at least, for the entangling power in the three-qubit cases we have computed with the magic matrix Z (see Sec. 7). The details will be presented in a forthcoming long paper.

As in the two-qubit case, both sides of Eq. (6) for a three-qubit gate is invariant under local unitary operations; that is, operators that can be written as $U(d_1) \otimes U(d_3)$, do not change the entangling power, as in [**20**], with $d_1 = 2$ and $d_3 = 4$.

6. Cartan decomposition for three qubits

We would like to use a recursive procedure that extends the Cartan decomposition to n qubits developed in [**13**]. Then we will work out the magic matrix (with n=3), to be used to compute the entangling power of three-qubit gates.

6.1. Direct Cartan decomposition of $SU(8)$. Consider the following decomposition of the Lie algebra $\mathfrak{su}(2^n)$:

$$\begin{aligned} \mathfrak{su}(2^n) &= span\{\sigma_x \otimes A, \sigma_y \otimes B, \sigma_z \otimes C, D \otimes \mathbb{1}, \\ &\quad i\sigma_{1x}, i\sigma_{1y}, i\sigma_{1z} \,\big|\, A, B, C, D \in \mathfrak{su}(2^{n-1})\} \\ \mathfrak{su}_{\mathfrak{l}}(2^n) &= span\{\sigma_z \otimes A, \mathbb{1} \otimes B, \\ &\quad i\sigma_{1z} \,\big|\, A, B \in \mathfrak{su}(2^{n-1})\} \\ \mathfrak{su}_{\mathfrak{m}}(2^n) &= span\{\sigma_x \otimes A, \sigma_y \otimes B, \\ &\quad i\sigma_{1x}, i\sigma_{1y} \,\big|\, A, B \in \mathfrak{su}(2^{n-1})\}, \end{aligned}$$

where $\sigma_{ix},\ \sigma_{iy},\ \sigma_{iz}$ are the Pauli matrices in the i^{th} qubit.

Lemma 1 The vector space $\mathfrak{su}_{\mathfrak{l}}(2^n)$ is a Lie subalgebra of $\mathfrak{su}(2^n)$, and $\mathfrak{su}(2^n) = \mathfrak{su}_{\mathfrak{l}}(2^n) \oplus \mathfrak{su}_{\mathfrak{m}}(2^n)$ is a Cartan decomposition; namely $\mathfrak{su}_{\mathfrak{l}}(2^n)$ and $\mathfrak{su}_{\mathfrak{m}}(2^n)$ satisfy the symmetric space commutation relations (8).

Lemma 2 We have $\exp(\mathfrak{su}_{\mathfrak{l}}(2^n)) = U(1) \otimes SU(2^{n-1}) \otimes SU(2^{n-1})$, of $SU(2^n)$.

From these two lemmas, it follows that

Theorem 1 Any element $U \in SU(2^n)$ admits a Cartan decomposition: $U = K_1 Z K_2$, where $K_1, K_2 \in U(1) \otimes SU(2^{n-1}) \otimes SU(2^{n-1})$ and $Z = \exp(Y) \subset G$ for some $Y \in \mathfrak{h}$, with $\mathfrak{h}$ a Cartan (maximal and abelian) subalgebra contained in $\mathfrak{su}_{\mathfrak{m}}(2^n)$.

We can choose the Cartan subalgebra for the matrix Z for the $n = 3$ case as follows.

Theorem 2 The vector space

$$\begin{aligned}\mathfrak{h} = span\{&\sigma_x \otimes \sigma_x \otimes \sigma_x, \sigma_y \otimes \sigma_y \otimes \sigma_x, \\ &\sigma_y \otimes \sigma_x \otimes \sigma_y, \sigma_x \otimes \sigma_y \otimes \sigma_y\}\end{aligned}$$

is a Cartan subalgebra contained in $\mathfrak{su}_{\mathfrak{m}}(8)$ (or that of the Lie algebra pair $(\mathfrak{su}(8), \mathfrak{su}_{\mathfrak{l}}(8))$).

Proof The proof consists of two parts. First, we must show that the basis elements shown above commute with each other. Second, we must show that no other members of $\mathfrak{su}_{\mathfrak{m}}(8)$ commute with all elements of this set. Hence, it is maximally abelian.

The first part is straightforward to check. To prove the second part, we need to first list the elements of the set that generates $\mathfrak{m}$:

$$\begin{aligned}\mathfrak{su}_{\mathfrak{m}}(8) \;=\; &span\{\sigma_x \otimes A, \sigma_y \otimes B, \\ &i\sigma_{1x}, i\sigma_{1y} \,\big|\, A, B \in \mathfrak{su}(4)\},\end{aligned}$$

and then explicitly check the relevant commutation relations.

Since we wish to calculate the entangling power over a bipartite split between the first and the other two qubits, it will be invariant with respect to the local $SU(2) \otimes SU(4)$ operations. We note that some operators in $\mathfrak{su}_{\mathfrak{l}}(8)$ are still non-local, i.e. do not belong to $SU(2) \otimes SU(4)$, so we need to further decompose $\mathfrak{su}_{\mathfrak{l}}(8)$ to isolate the non-local operators that are beyond $SU(2) \otimes SU(4)$. Eventually, we would like to capture all non-local entangling operations with an appropriately defined magic matrix. This will be carried out in next section.

6.2. Further Decomposition of $\mathfrak{su}_{\mathfrak{l}}$. There are operators in $\mathfrak{su}_{\mathfrak{l}}(8)$ that are capable of changing the entangling power, so that the matrix Z in Theorem 1, above, is incomplete as the magic matrix for three qubits. Our strategy is to make a further Cartan decomposition [**13**] for $\mathfrak{su}_{\mathfrak{l}}(8)$, to incorporate more entangling generators into an appropriate magic matrix.

First we note that σ_{1z} in $\mathfrak{su}_{\mathfrak{l}}(2^n)$ generates a U(1) subgroup, so we need to separate it: $\mathfrak{su}_{\mathfrak{l}}(2^n) = \mathfrak{u}(1) \oplus \overline{\mathfrak{su}_{\mathfrak{l}}(2^n)}$, and $\overline{\mathfrak{su}_{\mathfrak{l}}(2^n)}$ is semi-simple. We Cartan-decompose the latter as follows:

$$\begin{aligned}\overline{\mathfrak{su}_{\mathfrak{l}}(2^n)} \;&=\; span\{\sigma_z \otimes A, \mathbb{1} \otimes B \,\big|\, A, B \in \mathfrak{su}(2^{n-1})\} \\ \mathfrak{su}_{\mathfrak{l}1}(2^n) \;&=\; span\{\sigma_z \otimes A \,\big|\, A \in \mathfrak{su}(2^{n-1})\} \\ \mathfrak{su}_{\mathfrak{l}0}(2^n) \;&=\; span\{\mathbb{1} \otimes A \,\big|\, A \in \mathfrak{su}(2^{n-1})\},\end{aligned}$$

They satisfy the commutation relations (8).

In this way we end up with a decomposition of an SU(8) operator U that looks like

$$\begin{aligned}U \;&=\; K_1 Z K_2 \\ &=\; L_1\ A_1\ L_2\ Z\ L_3\ A_2\ L_4,\end{aligned}$$

where $L_i \in U(1) \otimes SU(4)$, K_i are generated from $\mathfrak{su}_{\mathfrak{l}}(2^n)$, Z is generated from the Cartan subalgebra of the pair $(\mathfrak{su}(2^n), \mathfrak{su}_{\mathfrak{l}}(2^n))$, and A_i are generated from the Cartan subalgebra of the pair $(\overline{\mathfrak{su}_{\mathfrak{l}}(2^n)}, \mathfrak{su}_{\mathfrak{l}0}(2^n))$.

We have shown in the previous section that the entangling power is invariant under the action of $K_i \in SU(2) \otimes SU(4)$. Now we would like to construct the magic matrix from the non-local A_i and Z. One is tempted to add to Z the generators of a Cartan subalgebra

$$\mathfrak{f} = span\{\sigma_z \otimes \mathbb{1} \otimes \sigma_z, \sigma_z \otimes \sigma_z \otimes \mathbb{1}, \sigma_z \otimes \sigma_z \otimes \sigma_z\}.$$

for the pair $(\overline{\mathfrak{su}_{\mathfrak{l}}(2^n)}, \mathfrak{su}_{\mathfrak{l}0}(2^n))$ that generates A_i. However, not all these generators commute with the generators of Z. Thus, we arrive at an (augmented) magic matrix:

$$\begin{aligned} M = & e^{-i(c_8\sigma_z\otimes\sigma_z\otimes\sigma_z)} \\ & \times e^{-i(c_1\sigma_x\otimes\sigma_x\otimes\sigma_x+c_2\sigma_y\otimes\sigma_y\otimes\sigma_x+c_3\sigma_y\otimes\sigma_x\otimes\sigma_y+c_4\sigma_x\otimes\sigma_y\otimes\sigma_y+c_5\sigma_z\otimes\sigma_{\mathbb{1}}\otimes\sigma_z+c_6\sigma_z\otimes\sigma_z\otimes\sigma_{\mathbb{1}})} \\ & \times e^{-i(c_7\sigma_z\otimes\sigma_z\otimes\sigma_z)} \end{aligned}$$

which is of the of the form

$$\begin{pmatrix} \omega_1 & 0 & 0 & 0 & 0 & 0 & 0 & \omega_7 \\ 0 & \omega_5 & 0 & 0 & 0 & 0 & \omega_3 & 0 \\ 0 & 0 & \omega_9 & 0 & 0 & \omega_{15} & 0 & 0 \\ 0 & 0 & 0 & \omega_{13} & \omega_{11} & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega_{12} & \omega_{14} & 0 & 0 & 0 \\ 0 & 0 & \omega_{16} & 0 & 0 & \omega_{10} & 0 & 0 \\ 0 & \omega_4 & 0 & 0 & 0 & 0 & \omega_6 & 0 \\ \omega_8 & 0 & 0 & 0 & 0 & 0 & 0 & \omega_2 \end{pmatrix}$$

where the non-vanishing entries ω_α $(\alpha = 1, 2, \cdots, 16)$ are expressed in terms of the sine and cosine functions of c_i $(i = 1, 2, \cdots, 8)$.

7. Three-qubit entangling power

We would like to calculate the entangling power of this magic matrix, as we did for the bipartite magic matrix.

From the cyclical property of the trace and the invariance of the entangling power [**20, 19**], $e_p[(U_1 \otimes U_3)\ U] = e_p(U)$ with $U_i \in U(d_i)(i = 1, 3)$, we have

$$\begin{aligned} e_p(U) &= e_p(L_1\ A_1\ L_2\ Z\ L_3\ A_2\ L_4) \\ &= e_p(A_1\ Z\ A_2) = e_p(M), \end{aligned}$$

which justifies construction of the magic matrix by throwing out the L_i.

Here we only present the resulting entangling power obtained from Eq. (6) for c_i $(i = 1, 2, \cdots, 6)$ non-vanishing, which include the GHZ and Werner states:

$$\begin{aligned} e_p(U) = \frac{1}{2}\Big\{1 \quad - \quad & \frac{1}{18}\big[\cos 4(c_1 - c_4)\cos 4(c_2 + c_3) \\ & + \cos 4(c_1 + c_4)\cos 4(c_2 + c_3) \\ & + \cos 4(c_2 + c_3)\cos 4(c_5 + c_6) \\ & + \cos 4(c_1 - c_4)\cos 4(c_5 + c_6) \\ & + \cos 4(c_2 - c_3)\cos 4(c_5 - c_6) \\ & + \cos 4(c_1 + c_4)\cos 4(c_5 - c_6)\big] \\ - \quad & \frac{1}{9}\big[\cos 4(c_1)\cos 4(c_3) + \cos 4(c_1)\cos 4(c_6) \\ & + \cos 4(c_2)\cos 4(c_4) + \cos 4(c_2)\cos 4(c_5) \\ & + \cos 4(c_3)\cos 4(c_6) + \cos 4(c_5)\cos 4(c_4)\big]\Big\}. \end{aligned}$$

This expression is maximal at $e_p = 2/3$ for $\{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8\} = \{\pi/4, \pi/4, 0, \phi, 0, 0, 0, 0\}$, with $0 \leq \phi \leq \pi/4$, $\pi/2$ periodic around $\pi/4$. With a maximal choice of parameters and $\phi = 0$, we get the Werner gate $\mathcal{W}$, that produces entangled Werner states from a sum of computational basis states. (Werner states satisfy $(U \otimes U \otimes U)\rho = \rho(U \otimes U \otimes U)$ for unitary operators U on $\mathcal{H}$, as defined in [**11**].) We leave to future study to check whether Eq. (6) with the new swap (14) is valid when c_7 and c_8 are non-zero.

7.0.1. *Three-qubit partial magic matrix Z.* With the Cartan subalgebra, $\mathfrak{h}$, we can form a three-qubit partial magic matrix. The Cartan subalgebra is not unique, and was chosen in this case to generate the magic matrix whose eigenstates are the GHZ states.

$$Z = e^{-i(c_1\sigma_x\otimes\sigma_x\otimes\sigma_x + c_2\sigma_y\otimes\sigma_y\otimes\sigma_x + c_3\sigma_y\otimes\sigma_x\otimes\sigma_y + c_4\sigma_x\otimes\sigma_y\otimes\sigma_y)}$$

$$= \begin{pmatrix} c^1 & 0 & 0 & 0 & 0 & 0 & 0 & -is^1 \\ 0 & c^{-2} & 0 & 0 & 0 & 0 & -is^{-2} & 0 \\ 0 & 0 & c^4 & 0 & 0 & is^4 & 0 & 0 \\ 0 & 0 & 0 & c^3 & is^3 & 0 & 0 & 0 \\ 0 & 0 & 0 & is^3 & c^3 & 0 & 0 & 0 \\ 0 & 0 & is^4 & 0 & 0 & c^4 & 0 & 0 \\ 0 & -is^{-2} & 0 & 0 & 0 & 0 & c^{-2} & 0 \\ -is^1 & 0 & 0 & 0 & 0 & 0 & 0 & c^1 \end{pmatrix}$$

where $c^1 = \cos(c_1 - c_2 - c_3 - c_4)$, $c^{-2} = \cos(c_1 - c_2 + c_3 + c_4)$, . . . , $s^4 = \sin(-c_1 - c_2 - c_3 + c_4)$, and so on.

This has an analogous maximally entangled eigenbasis, i.e. a magic basis with global phases to maintain concurrence properties (see for example [**15**]). The basis states are

$$
\begin{aligned}
\big|\Phi_1\big\rangle &= \tfrac{e^{-i\frac{\pi}{3}}}{\sqrt{2}}(\big|000\big\rangle + \big|111\big\rangle) \qquad \big|\Phi_8\big\rangle = \frac{e^{i\frac{\pi}{6}}}{\sqrt{2}}(\big|000\big\rangle - \big|111\big\rangle)\\
\big|\Phi_2\big\rangle &= \tfrac{e^{-i\frac{\pi}{3}}}{\sqrt{2}}(\big|001\big\rangle - \big|110\big\rangle) \qquad \big|\Phi_7\big\rangle = \frac{e^{i\frac{\pi}{6}}}{\sqrt{2}}(\big|001\big\rangle + \big|110\big\rangle)\\
\big|\Phi_3\big\rangle &= \tfrac{e^{i\pi}}{\sqrt{2}}(\big|010\big\rangle + \big|101\big\rangle) \qquad \big|\Phi_6\big\rangle = \frac{e^{i\frac{\pi}{2}}}{\sqrt{2}}(\big|010\big\rangle - \big|101\big\rangle)\\
\big|\Phi_4\big\rangle &= \tfrac{e^{i\pi}}{\sqrt{2}}(\big|011\big\rangle - \big|100\big\rangle) \qquad \big|\Phi_5\big\rangle = \frac{e^{i\frac{\pi}{2}}}{\sqrt{2}}(\big|011\big\rangle + \big|100\big\rangle).
\end{aligned}
$$

7.1. Entangling power of GHZ generators. Here we present another method to compute the entangling power of the GHZ generators by unitary transformation U_t between the magic matrix and GHZ generators.

Consider, say, the matrices $B_{8,2}$ and $B_{8,3}$, which are generators of the GHZ states given in Ref. [**7**]

$$
B_{8,2} = \frac{1}{\sqrt{2}}\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0\\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 1 & 0 & 0 & 0\\
0 & 0 & -1 & 0 & 0 & 1 & 0 & 0\\
0 & -1 & 0 & 0 & 0 & 0 & 1 & 0\\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix},
$$

$$
B_{8,3} = \frac{1}{\sqrt{2}}\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 0 & -1 & 0\\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 1 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0\\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
$$

To find U_t, below, we transform the eigenstates from the GHZ states to the magic states. It amounts to transforming the bases for the diagonalized forms of the operators. So, the unitary matrix to transform the GHZ generator $B_{8,2}$ to the magic matrix is,

$$
\begin{aligned}
U_t &= \begin{pmatrix}
e^{-i\frac{\pi}{3}} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & e^{-i\frac{\pi}{3}} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & e^{i\pi} & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & e^{i\pi} & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & e^{i\frac{\pi}{2}} & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & e^{i\frac{\pi}{2}} & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & e^{i\frac{\pi}{6}} & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & e^{i\frac{\pi}{6}}
\end{pmatrix}\\
&= \begin{pmatrix} e^{-i\frac{5\pi}{12}} & 0 \\ 0 & e^{i\frac{5\pi}{12}} \end{pmatrix} \otimes \begin{pmatrix} e^{i\frac{\pi}{12}} & 0 \\ 0 & e^{-i\frac{7\pi}{12}} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}
$$

U_t transforms the GHZ matrix to the magic matrix, with constants $c_2 = \pi/4$ and $c_1 = c_3 = c_4 = c_5 = c_6 = 0$, within the bounds for maximum entangling power for $c_1 = 0$. However, this is not maximal in general. U_t for $B_{8,3}$ is nearly the same and ends up with the same results, with both the second and seventh, and the third and sixth, diagonal entries of U_t to be swapped.

Of course, this choice of constants is immediately obvious from the eigenvalues of these operator matrices. They can be read directly from the generator form of these operators, especially in this case where these generators are potential members of a Cartan subalgebra:

$$B_{8,1} = e^{i\frac{\pi}{4}\sigma_x^{\otimes 2}\otimes\sigma_y}$$
$$B_{8,2} = e^{i\frac{\pi}{4}\sigma_y\otimes\sigma_x^{\otimes 2}}$$
$$B_{8,3} = e^{-i\frac{\pi}{4}\sigma_y^{\otimes 3}}.$$

8. Conclusion

Our original motivation has been to calculate the entangling power of some braiding operators, including the GHZ generators. To this end, we have extended the magic matrix method to SU(8) for three qubits. To calculate the entangling power of a unitary operator, it is necessary only to know the eigenvalues, up to a global phase. One compares these eigenvalues to the eigenvalues of the magic matrix to determine the constants that appear in the entangling power formula (10).

We have found that the GHZ generators in which we were originally interested, are not maximally entangling. Instead, another choice of parameters yields maximally entangling operators, one of which we have shown generates Werner states from the initial uniform product state.

Finally we note that our formalism of the recursive Cartan decomposition suggests that information of entangling power, as captured by the parameters of the operators in the Cartan subalgebra, is encoded in roughly of order $\mathrm{O}(2^n)$ constants for operators in $\mathrm{SU}(2^n)$. Used in conjunction with entanglement combing, this could be a useful criterion of the success of multiparty protocols such as multipartite quantum communication, multipartite teleportation, and distributed compression.

Acknowledgements One of the authors, YSW, thanks Prof. Kazem Mahdavi and other organizers, and the Department of Computer Science in University of Texas at Tyler for the invitation and for the warm hospitality during the wonderful workshop. YSW's work was supported in part by US NSF through grant PHY-0756958.

References

[1] P.K. Aravind, *Borromean entanglement in the GHZ state*, in *Potentialilty, Entanglement and Passion-at-a-Distance*, Cohen, Robert S., Michael Horne and John Stachel (eds.), Kuluwer Academic Publishers, Boston 1997, 53-59.

[2] Louis H. Kauffman and Samuel J. Lomonaco Jr., *Braiding operators are universal quantum gates*, arXiv:quant-ph/0401090.

[3] M.H. Freedman, A. Kitaev, and Z. Wang, *Simulation of topological field theories by quantum computers*, Commun. Math. Phys. **227**(587), 2002.

[4] M.H. Freedman, A. Kitaev, M. Larsen and Z. Wang, *Topological Quantum Computation*, Bull. Amer. Math. Soc. (N.S.) **40** (31), 2003.

[5] Zhenghan Wang, *Topoligical Quantum Computation*, Conference Board of the mathematical Sciences, No. 112 (American Mathematical Society), 2010.
[6] Y. Zhang and M.L. Ge, *GHZ States, Almost-Complex Structure and Yang–Baxter Equation*, accepted by Quant. Inf. Proc. for publication. arXiv: quant-ph/0701244.
[7] E. C. Rowell, Y. Zhang, Y.S. Wu and M.L. Ge. *From extraspecial two-groups to GHZ states*. arXiv:quant-ph/0706.1761, 2007.
[8] J.L. Chen, K. Xue and M.L. Ge, "Berry phase and quantum criticality in Yang–Baxter systems", Ann. Phys. **323** (2614), 2008.
[9] A. Datta. *Studies on the role of entanglement in mixed-state quantum computation*. PhD thesis, The University of New Mexico, August 2008.
[10] A. Datta, S. T. Flammia, and C. M. Caves. *Entanglement and the power of one qubit*. Phys. Rev. A, **72**(042316), 2005.
[11] T. Eggeling and R. F. Werner. *Separability properties of tripartite states with $u \otimes u \otimes u$ symmetry*. Phys. Rev. A, **63**(042111), 2001.
[12] S. Helgason. *Differential Geometry, Lie Groups, and Symmetric Spaces (Graduate Studies in Mathematics)*. American Mathematical Society, 2001.
[13] N. Khaneja and S. J. Glaser. *Cartan decomposition of $su(2^n)$, constructive controllability of spin systems, and universal quantum computing*. arXiv:quant-ph/0010100, 2000.
[14] B. Kraus and J. Cirac. *Optimal creation of entanglement using a two-qubit gate*. Phys. Rev. A, **63**(062309), 2001.
[15] A. Rezakhani. *Characterization of two-qubit perfect entanglers*. Phys. Rev. A, **70**(052313), 2004.
[16] J. A. Wolf. *Spaces of Constant Curvature*. Publish or Perish, Inc., 1984.
[17] D. Yang and J. Eisert. *Entanglement combing*. Phys. Rev. Lett., **103**(220501), 2009.
[18] M.-Y. Ye, D. Sun, Y.-S. Zhang, and G.-C. Guo. *Entanglement changing power of two-qubit unitary operations*. arXiv:quant-ph/0403163, 2004.
[19] P. Zanardi. *Entanglement of quantum evolutions*. Phys. Rev. A, **63**(040304(R)), 2001.
[20] P. Zanardi, C. Zalka, and L. Faoro. *On the entangling power of quantum evolutions*. Phys. Rev. A, **62**(030301), 2000.
[21] L. Clarisse, S. Ghosh, S. Severini, and A. Sudbery. *Entangling power of pemutations*. Phys. Rev. A, **72**(012314), 2005.
[22] S. Hill and W. K. Wootters. *Entanglement of a pair of quantum bits*. Phys. Rev. Lett., **78**(26), 1997.
[23] N. Khaneja, R. Brockett, and S. J. Glaser. *Time optimal control in spin systems*. Phys. Rev. A, **63**(032308), 2001.
[24] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley. *Geometric theory of nonlocal two-qubit operations*. Phys. Rev. A, **67**(042313), 2003.
[25] D. DiVincenzo. *The Physical Implementation of Quantum Computation*. Fortschr. Phys., 48:9, 2000.
[26] Y. Zhang, L. H. Kauffman, and M.-L. Ge. *Yang-baxterizations, universal quantum gates, and hamiltonians*. arXiv:quant-ph/0502015, 2005.
[27] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley. *Minimum Construction of Two-Qubit Quantum Operations*. Phys. Rev. Lett., **93**(020502), 2004.

Department of Physics and Astronomy, University of Utah, Salt Lake City, Utah 84112, U.S.A.
E-mail address: adballar@physics.utah.edu

Department of Physics and Astronomy, University of Utah, Salt Lake City, Utah 84112, U.S.A.
E-mail address: wu@physics.utah.edu

This page intentionally left blank

Contemporary Mathematics
Volume **536**, 2011

A Unified Approach to Universality for Three Distinct Types of 2-qubit Quantum Computing Devices

Goong Chen, Viswanath Ramakrishna, and Zhigang Zhang

Abstract. The universality of entangling 2-bit operations for three types of quantum computing devices which is usually established in an ad hoc way, is, in this work, given a *unified treatment*. The key observation is that these various Hamiltonians can be made conjugate to each other, up to an insignificant phase factor. Furthermore, these unitary conjugations can be obtained without any recourse to eigenvector-eigenvalue computations. The chief enabling tool for this is the realization that these three Hamiltonians belong to Cartan subalgebras of three Cartan decompositions of $su(4)$ that are all of the same type. The three physical systems considered here are cavity-QED, quantum dots, and a SQUID of charge-flux type.

1. Introduction

The purpose of this paper is twofold. First, we provide an exposition of certain universality results for quantum computation and the physical architectures of three types of vehicles for quantum computation, i.e., cavity-QED, ion traps and SQUIDS of charge flux type. We then show their *diagonalization* process (without the need of calculating eigenvalues and eigenvectors) such that these three systems are closely related, implying an equivalent cavity-QED design (which by its very nature is *diagonal*). In the process, we show yet another application of Lie algebraic notions to the engineering of quantum systems.

It turns out that these 3 systems admit a unified treatment, a point which, to the best of our knowledge, has not been recognized in the literature. The key fact which leads us to this important observation is that the Hamiltonians describing these systems, whilst not having the same set of eigenvalues, have the *the same eigenvalue multiplicity (degeneracy) structure.* This then yields unitary conjugations, up to an overall phase factor, between these three Hamiltonians.

Given the considerable physical importance of these three systems going even beyond quantum computation, the fact that they are related in a very precise fashion is of significance. We speculate that the fact that these 3 Hamiltonians do

1991 *Mathematics Subject Classification.* 81QXX,81RXX,22EXX,94AXX,94CXX.

Key words and phrases. Universality, Cavity-QED, Quantum Dots, SQUIDS, Cartan Decompositions.

Supported in part by Texas ARP Grant 010366-0149-2009 and QNRP Grant NPRP 09-462-1-074.

not have identical spectra may have caused this relationship to be missed in the literature.

Not only are there unitary conjugations (up to phase) between these 3 systems, but they can also be written down in closed form without having to compute normalized eigenvectors. The key to this is the observation that each of these Hamiltonians is a linear combination of three commuting linearly independent terms, and three is precisely the rank of the so-called Type I Cartan decomposition of the Lie algebra $su(4)$. This makes it plausible that these three Hamiltonians belong to the Cartan subalgebras of three Cartan decompositions of $su(4)$, all of which are conjugate to one another. This is indeed the case, and therefore the unitary conjugations between these three Hamiltonians can be taken to be the unitary conjugations which render these three Type I Cartan decompositions conjugate.

Of course, unitary conjugations are not unique and one can always question whether the invocation of the theory of Cartan decompositions can be avoided. We have chosen its invocation for two reasons. First, this has the benefits of being constructive and explicit, and it was indeed how we obtained these specific conjugations and therefore merely writing down these conjugations would have seemed *ad hoc* or suggested that these were obtained by eigenvector calculations, which is manifestly incorrect. Indeed, it is by appealing to this theory that we were able to immediately recognize that one of the conjugations can be taken to be the magic basis matrix (a matrix which shows up in several situations in the quantum computing literature) and that the second can always be taken to be a real orthogonal matrix, as opposed to a general unitary matrix. Second, the theory of Cartan decompositions is of great relevance to a variety of topics in quantum engineering (e.g., the theory of concurrence, quantum control, mutually unbiased bases), and therefore it should be part of the repertoire of any practitioner of this field. Indeed, it holds the promise of being generalizable to potentially much intricate multi-qubit quantum computing circuits. Proving the property of being an *entangling* operation can be done in many ways without the need of Lie–Cartan theory for multi-qubit cases (see Zanardi et al. [**8**], e.g.). However, finding some inherent mathematical conjugations and performing blockwise diagonalizations need the Lie–Cartan theory almost as an indispensable tool.

1.1. Some basic universality theorems.

Various quantum computing devices have been proposed for the construction of the future quantum computer. Most prominent proposals among them are cavity-QED, ion traps, atom traps, quantum dots, linear optics, SQUID (superconducting quantum interference devices), liquid and solid state NMR, etc., cf. [**4**]. An absolute requisite on any quantum computing device is that it must be able to perform *universal quantum gate operations*. Thus, we begin our paper by stating some basic theorems on universal quantum gates.

THEOREM 1.1 (DiVincenzo [**6**]). *The collection of all 1-bit and 2-bit unitary quantum gates are universal for quantum computing. In fact, the collection of all 1-bit gates, plus the (Control-Not) CNOT 2-bit gate, are universal.* □

A theorem, equivalent to DiVincenzo's Theorem 1.1 above, is favored by mathematicians. We state it as follows.

THEOREM 1.2 (J.-L. Brylinski and R. Brylinski [**1**]). *Let V be a given 2-bit gate. Then the following are equivalent:*

(i) *The collection of all 1-bit gates A together with V is universal;*
(ii) *V is imprimitive, namely, for any 1-bit gates S and T,*

$$V \neq S \otimes T, \quad V \neq (S \otimes T)U_{\text{swap}},$$

where U_{swap} is the 2-bit swap gate defined by

$$U_{\text{swap}}|ij\rangle = |ji\rangle, \qquad i, j \in \{0, 1\}. \tag{1.1}$$

□

Another refined theorem, again due to J.-L. Brylinski and R. Brylinski [**1**], may be stated as follows.

THEOREM 1.3 ([1, Theorem 4.4]). *The collection of all 1-bit gates $U_{\theta,\phi}$:*

$$U_{\theta,\phi} \equiv \begin{bmatrix} \cos\theta & -ie^{-i\phi}\sin\theta \\ -ie^{-i\phi}\sin\theta & \cos\theta \end{bmatrix}, \qquad 0 \leq \theta, \phi \leq 2\pi, \tag{1.2}$$

together with any (single) 2-bit gate

$$Q_\eta \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\eta} \end{bmatrix}, \qquad 0 < \eta < 2\pi, \tag{1.3}$$

is universal. □

The gate $U_{\theta,\phi}$ in (1.2) is called a *Rabi rotation gate*, while Q_η in (1.3) is called a *quantum phase gate*. In the design of quantum circuits, computer scientists seem to prefer the use of the CNOT-gate obviously due to its logical connotations, while physicists generally like to use the Q_η gates because they are more directly related to the function of certain physical devices such as the cavity-QED. The equivalence or exchangeability between CNOT and Q_π can be seen from Fig. 1.

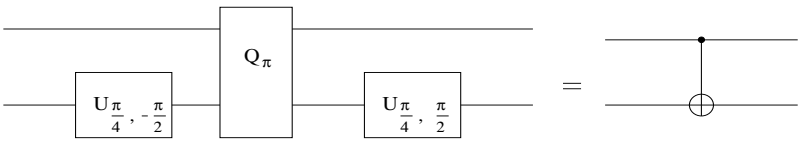


FIGURE 1. The equality of the above two quantum circuits signifies the identity CNOT $= U^{(2)}_{\pi/4,\pi/2} Q_\pi U^{(2)}_{\pi/4,-\pi/2}$, where the superscript (2) on U denotes that the action is on the second qubit.

Based on the above understanding, we see that for any specific type of quantum devices, in order to prove that it is indeed universal, we need to establish that it can perform $U_{\theta,\phi}$ ($0 \leq \theta, \pi \leq 2\pi$) 1-bit operations as well as 2-bit Q_η (for $\eta \neq 2\pi$) or CNOT operations. The availability of the 1-bit rotation gates $U_{\theta,\phi}$ is usually "straightforward". Thus, the main issue of universality becomes actually a test of whether a 2-bit quantum gate operation can *generate quantum entanglement* (such as CNOT or Q_π does) or not. Thus, our goal in this paper is to investigate such 2-bit entangling operations for some quantum devices. Our hope is to achieve a *unified treatment* of universality for many different types of devices. Previously, as we have seen in [**4**], the universality of quantum computing devices was established in an *ad hoc* way. This effort first started in an earlier paper by the three of us [**9**].

However, the use of the Lie–Cartan theory here substantially simplifies the finding of the requisite conjugations.

In the forthcoming sections of our paper, the organization is made as follows. In Section 2, we describe the Hamiltonians of the quantum computing devices to be treated: cavity-QED, quantum dots and a SQUID of the charge-flux type. In Section 3, we review the requisite Lie algebra and Cartan decomposition theorems and apply them to the diagonalization of the Hamiltonian operators corresponding to the given quantum computing devices. Brief conclusions are given at the end of the paper.

2. Hamiltonians for cavity-QED, quantum dots and SQUID (2-bit operations)

Quantum devices' actions in the theory of quantum computing can be modeled by their *Hamiltonians*. The cornerstone of quantum mechanics is the Schrödinger equation

$$\begin{cases} i\hbar\dfrac{\partial}{\partial t}\psi(\boldsymbol{r},t) = H\psi(\boldsymbol{r},t), \quad t>0, \boldsymbol{r}\in\mathbb{R}^N, \\ \psi(\boldsymbol{r},0) = \psi_0(\boldsymbol{r}) \qquad\qquad \text{(the initial condition)}, \end{cases} \tag{2.1}$$

where H is a self-adjoint partial differential operator called the Hamiltonian of the system. H consists of the kinetic energy part:

$$\mathcal{K} = -\sum_{k=1}^{n}\frac{\hbar^2}{2m_k}\nabla_k^2 \qquad \left(\nabla_k^2 = \frac{\partial^2}{\partial x_{k,1}^2}+\frac{\partial^2}{\partial x_{k,2}^2}+\frac{\partial^2}{\partial x_{k,3}^2}\right), \tag{2.2}$$

and the potential energy part

$$\mathcal{P} = V(\boldsymbol{r}_1,\boldsymbol{r}_2,\ldots,\boldsymbol{r}_n)\cdot \tag{2.3}$$

where $\boldsymbol{r}_k = (x_{k,1},x_{k,2},x_{k,3})$ denotes the position of the k^{th} particle, $m_k>0$ is the mass of the k^{th} particle, n is the total number of particles, and $N=3n$. The potential energy operator $\mathcal{P}$ in (2.3) may take various forms, depending on the physics to be modeled. Equation (2.1) is usually posed on an infinite dimensional Hilbert space. Closed-form solutions of (2.1) are unavailable for most cases. Nevertheless, under special or idealized conditions, solutions of (2.1) are known to lie in a finite-dimensional invariant subspace, and simplifications of (2.1) become possible in that subspace, resulting in a *reduced-order model*. Here, we pick out three of such models as subjects for discussion:

(a) **Cavity-QED**: Its effective interaction Hamiltonian is given by

$$H_{\text{CQED}} = -\frac{\hbar g^2}{\Delta}(aa^\dagger|\alpha\rangle\langle\alpha| - a^\dagger a|\beta\rangle\langle\beta|), \quad \text{(cf. [4, p. 128, (3.90)])} \tag{2.4}$$

on the invariant (Hilbert) subspace

$$\mathcal{H} = \text{span}\{|\gamma,0\rangle,|\gamma,1\rangle,|\beta,0\rangle,|\beta,1\rangle\}, \tag{2.5}$$

where $|\gamma\rangle$ is the state in Fig. 2 that is *detached* (or off-resonance) from the two levels $|\alpha\rangle$ and $|\beta\rangle$. The second qubit in (2.5) represents the photon number inside the cavity; $a, a^\dagger$ are, respectively, the annihilation and creation operators on the photon number states; g is the coupling constant,

and $\Delta \equiv \nu - \omega_{\alpha\beta}$ is the detuning frequency. Note that we may identify $|1\rangle = |\beta\rangle$ and $|0\rangle = |\gamma\rangle$ in (2.5) so that (2.5) becomes

$$\mathcal{H} = \text{span}\{|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle\}, \tag{2.6}$$

the 2-qubit Hilbert space.

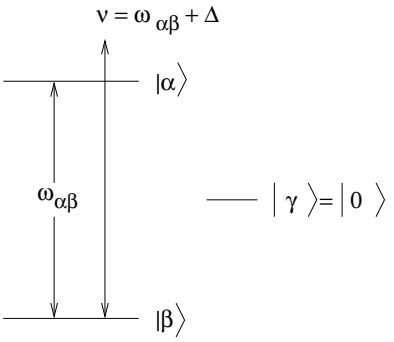


FIGURE 2. Atomic energy levels used in cavity QED related to equation (2.4). A 3-level $(|\alpha\rangle, |\beta\rangle, |\gamma\rangle)$ atom passes through a cavity. A strong electromagnetic (laser) field of the privileged cavity mode of frequency ν interacts with the atom. The cavity photons excite the electric dipole transition between $|\beta\rangle$ and $|\alpha\rangle$, leading to a phase shift for the qubit state $|\beta\rangle = |1\rangle$ under suitable conditions. The second qubit state $|\gamma\rangle = |0\rangle$ is unaffected by the cavity photons.

(b) **Quantum dots:** The Hamiltonian of a spintronics design due to Burkard, Engel and Loss [**5**] is

$$H = \sum_{j=1}^{n} \mu_B g_j(t) \boldsymbol{B}_j(t) \cdot S_j + \sum_{1 \le j < k \le n} J_{jk}(t) \boldsymbol{S}_j \cdot \boldsymbol{S}_k, \qquad \text{(cf. [4, p. 318, (7.14)])} \tag{2.7}$$

which is a 1-dimensional Ising (array) model, where the first summation denotes the sum of energy due to the application of the magnetic field $\boldsymbol{B}_j$ to the electron spin at dot j, while the second denotes the interaction Hamiltonian through the tunneling effect of a gate voltage applied between the dots, and $\boldsymbol{S}_j, \boldsymbol{S}_k$ are the spins of the electric charge quanta at, respectively, the j^{th} and k^{th} quantum dot. Cf. Fig. 3.

We confine our attention to the case of just two quantum dots and obtain from (2.7) the following:

$$H_{QD} = H_{QD}(t) = \omega(t) \boldsymbol{S}_1 \cdot \boldsymbol{S}_2 = \omega(t)[\sigma_x^{(1)} \otimes \sigma_x^{(2)} + \sigma_y^{(1)} \otimes \sigma_y^{(2)} + \sigma_z^{(1)} \otimes \sigma_z^{(2)}], \tag{2.8}$$

the 2-bit quantum dot Hamiltonian operator on the Hilbert space $\mathcal{H}$ in (2.6), where in (2.8), we have used the definition of the dyadic $\boldsymbol{S}_j = (\sigma_x^{(j)}, \sigma_y^{(j)}, \sigma_z^{(j)})$ for the j^{th} bit, $j = 1, 2$, with $\sigma_x^{(j)} = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, $\sigma_y^{(j)} = \left[\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right]$ and $\sigma_z^{(j)} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ as the standard Pauli matrices on the j^{th} bit.

The quantum-dot Hamiltonian $H_{QD}(t)$ as given by (2.8) is time-dependent. Nevertheless, we have the commutativity

$$H_{QD}(t_1) H_{QD}(t_2) = H_{QD}(t_2) H_{QD}(t_1), \text{ for any } t_1, t_2 \ge 0.$$

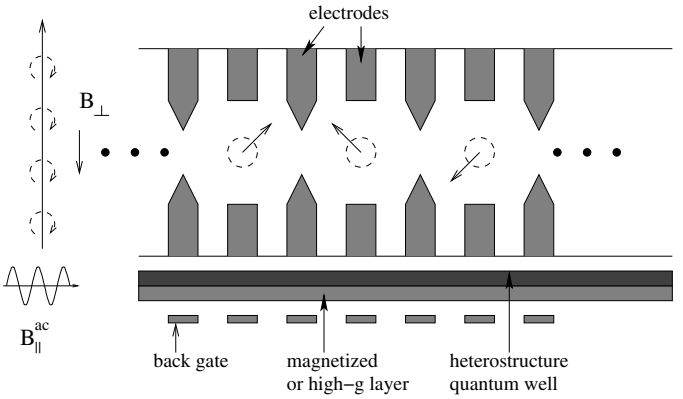


FIGURE 3. A linear array of laterally coupled quantum dots, based on the original schematic design in Burkard, Engel and Loss [**5**]. Each circle represents a quantum dot, where the arrow represents the spin-$\frac{1}{2}$ ground state of the confined electron. The electrodes (dark gray) confine single electrons to the dot regions (circles). The electrons can be moved by electrical gating into the magnetized or high-magnetic dipole moment layer to produce locally different Zeeman splittings.

Therefore, the corresponding evolution operator is given by

(2.9)
$$e^{-i\int_0^t H_{QD}(\tau)d\tau/\hbar} = \exp\left[-i\int_0^t \omega(\tau)d\tau(\sigma_x^{(1)}\otimes\sigma_x^{(2)} + \sigma_y^{(1)}\otimes\sigma_y^{(2)} + \sigma_z^{(1)}\otimes\sigma_z^{(2)})/\hbar\right],$$

and since $\omega(t)$ is tunable, (2.9) works essentially as the autonomous (i.e., time-independent) case whose evolution operator is given by

$$\exp[-it(\sigma_x^{(1)}\otimes\sigma_x^{(2)} + \sigma_y^{(1)}\otimes\sigma_y^{(2)} + \sigma_z^{(1)}\otimes\sigma_z^{(2)})/\hbar].$$

Thus, from now on, we just regard $\omega(t)\equiv\omega\in\mathbb{R}$ in (2.8) and denote

(2.10)
$$H_{QD} \equiv \omega[\sigma_x^{(1)}\otimes\sigma_x^{(2)} + \sigma_y^{(1)}\otimes\sigma_y^{(2)} + \sigma_z^{(1)}\otimes\sigma_z^{(2)}].$$

(c) **SQUID:** The Hamiltonian of a *dc*-SQUID with charge-flux qubits and inductance as shown in Fig. 4 is

(2.11)
$$H = -E_J^{(1)}\sigma_x^{(1)} - E_J^{(2)}\sigma_x^{(2)} + \Pi_{12}\sigma_x^{(1)}\otimes\sigma_x^{(2)} \qquad \text{cf. [4, p. 436, (9.83)]}.$$

This may be written a little bit more explicitly as

(2.12)
$$H = -E_J^{(1)}\sigma_x^{(1)}\otimes I^{(2)} - E_J^{(2)}I^{(1)}\otimes\sigma_x^{(2)} + \Pi_{12}\sigma_x^{(1)}\otimes\sigma_x^{(2)},$$

where $I^{(i)}$ is the identity operator on the i^{th} bit, for $i=1,2$. Further, let us only consider a special case of (2.12):

(2.13)
$$H_{\text{SQUID}} = \delta(-\sigma_x^{(1)}\otimes I^{(2)} - I^{(1)}\otimes\sigma_x^{(2)} + \sigma_x^{(1)}\otimes\sigma_x^{(2)})$$

where $\delta = E_J^{(1)} = E_J^{(2)} = \Pi_{12}$ holds. Once again, (2.13) is a Hamiltonian operator defined on the 2-bit Hilbert space $\mathcal{H}$ in (2.6).

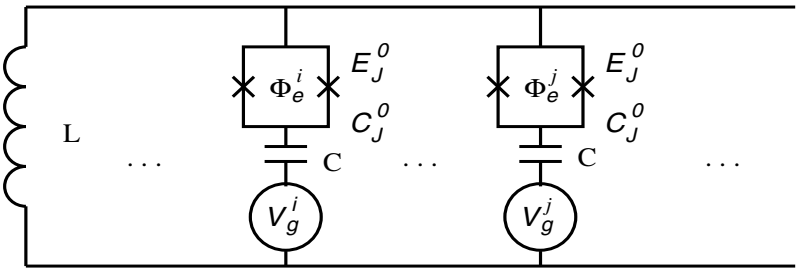


FIGURE 4. A design for coupling charge qubits with inductance where the junctions in the charge qubits are replaced by a dc-SQUID. C is capacitance and V_g is the applied voltage. All qubits are coupled through an inductor L, and an external field Φ_e^i penetrates every dc-SQUID. This changes the effective Josephson term in the Hamiltonian to $-2E_J^0 \cos(\pi\Phi_e/\Phi_0)\cos\phi$ and makes E_J tunable by Φ_e^i.

It is useful to remark that the conjugation to be produced later will also diagonalize the Hamiltonian of the **SQUID**, even without the assumption that $\delta = E_J^{(1)} = E_J^{(2)} = \Pi_{12}$.

The proofs that each of $H_{\mathrm{CQED}}, H_{\mathrm{QD}}$ and H_{SQUID} generates entangling 2-bit unitary operations can be found in [**4**, Chaps. 3, 7 and 9]. However, as stated earlier here our main interest is to find a *unified treatment* for these different devices.

REMARK 2.1. Two time-independent Hamiltonian operators H_1 and H_2 on the same Hilbert space $\mathcal{H}$ are said to be conjugate, *up to phase*, to each other if there exists a unitary transformation U on $\mathcal{H}$ such that

$$H_1 = kU^\dagger H_2 U, \text{ for some real } k \neq 0. \tag{2.14}$$

If (2.14) holds, then the evolution of the two quantum systems

$$i\hbar\frac{d}{dt}\psi^{(j)}(t) = H_j\psi^{(j)}(t), \qquad j = 1, 2,$$

are equivalent, up to phase, through the conjugacy

$$e^{-itH_1/\hbar} = e^{-ikt}U^\dagger e^{-itH_2/\hbar}U. \tag{2.15}$$

□

REMARK 2.2. The matrix representation of $H_{\text{CQED}}, H_{\text{QD}}$ ((2.10)) and H_{SQUID} with respect to the ordered basis in (2.6) are, respectively,

$$\begin{cases} H_{\text{CQED}} = E_0 \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad E_0 \equiv \hbar g^2/\Delta (\neq 0), \\ \text{Eigenvalues of } H_{\text{CQED}}\text{: } 0 \text{ (triplet)}, E_0 \cdot 1 \text{ (singlet)}; \end{cases} \tag{2.16}$$

$$\begin{cases} H_{\text{QD}} = \omega \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad (\omega \neq 0) \\ \text{Eigenvalue of } H_{\text{QD}}\text{: } \omega \cdot 1 \text{ (triplet)}, \omega \cdot (-3) \text{ (singlet)}; \end{cases} \tag{2.17}$$

$$\begin{cases} H_{\text{SQUID}} = \delta \begin{bmatrix} 0 & 1 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{bmatrix}, \qquad (\delta \neq 0), \\ \text{Eigenvalues of } H_{\text{SQUID}}\text{: } \delta \cdot 1 \text{ (triplet)}, \delta \cdot (-3) \text{ (singlet)}. \end{cases} \tag{2.18}$$

Obviously, H_{CQED} cannot be conjugate, in the usual sense of the word, to either H_{QD} or H_{SQUID} since their spectra differ. *On the other hand, the multiplicity (degeneracy) structures of their eigenvalues are identical, and this suggests that there is a close connection between these Hamiltonians.* Indeed, a simple transformation

$$\widetilde{H}_{\text{CQED}} \equiv E_0 \left(I_4 - \frac{4}{E_0} H_{\text{CQED}} \right) \tag{2.19}$$

(I_4 is the identity operator on $\mathcal{H}$)

gives

$$\begin{cases} \widetilde{H}_{\text{CQED}} = E_0 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 \end{bmatrix}, \\ \text{Eigenvalues of } \widetilde{H}_{\text{CQED}}\text{: } E_0 \cdot 1 \text{ (triplet)}, E_0 \cdot (-3) \text{ (singlet)}. \end{cases} \tag{2.20}$$

The evolution operator corresponding to $\widetilde{H}_{\text{CQED}}$ satisfies

$$e^{-i\widetilde{H}_{\text{CQED}} t/\hbar} = e^{-iE_0 t/\hbar} e^{4itH_{\text{CQED}}/\hbar}, \tag{2.21}$$

where $e^{-iE_0 t/\hbar}$ is only a scalar phase factor. Thus, $\exp(-i\widetilde{H}_{\text{CQED}} t/\hbar)$ is an entangling unitary operation if and only if $\exp(4itH_{\text{CQED}}/\hbar)$ is. We can, therefore, replace H_{CQED} with $\widetilde{H}_{\text{CQED}}$. Now, from (2.17), (2.18) and (2.20), it is almost clear that $\widetilde{H}_{\text{CQED}}, H_{\text{QD}}$ and H_{SQUID} are conjugate to each other through the observation of their eigenvalues. The exact nature of such conjugacies remains to be determined. This is the main task of Section 3. □

3. Cartan decompositions of $su(4)$ and the explicit conjugacies

In this section we provide explicit expressions for the conjugacies, whose existence is guaranteed by the considerations of the previous section. It is emphasized that these conjugacies are found *without any eigenvector calculations.* The key to this is to observe that both H_{QD} and H_{SQUID} are each the sum of *three* commuting,

linearly independent terms and that *three* is the rank of the Type I Cartan decomposition of $su(4)$, as will be clarified presently. To that end, a brief detour into the theory of Lie algebras (Cartan decompositions, in particular) is needed. This helps make the paper more self-contained, as the majority of the quantum computation and information researchers are not familiar with the theory of Cartan decompositions, which together with its variants actually plays an important role in many topics in quantum information theory.

Let us now give a quick summary of the results and notions needed. We refer the reader to [**7**], e.g., for further information.

DEFINITION 3.1. Let $\mathfrak{g}$ be a semisimple Lie algebra with Lie bracket $[\ ,\ ]$ and an inner product given by the Killing form $\langle\ ,\ \rangle$. A vector space direct sum decomposition of $\mathfrak{g}$ in the form

$$\mathfrak{g} = \widetilde{K} \oplus \widetilde{P}, \text{ where } \widetilde{P} \equiv \widetilde{K}^{\perp},$$

is called a Cartan decomposition of $\mathfrak{g}$ if

$$\begin{aligned} &[\widetilde{K}, \widetilde{K}] \subseteq \widetilde{K}, \text{ i.e., } \widetilde{K} \text{ is a Lie subalgebra,} \\ &[\widetilde{K}, \widetilde{P}] \subseteq \widetilde{P}, \text{ and } [\widetilde{P}, \widetilde{P}] \subseteq K. \end{aligned} \tag{3.1}$$

□

EXAMPLE 3.1. In general quantum mechanics, and in quantum computing and quantum information, the following Lie algebras and Lie groups are often used:

$$\begin{aligned} su(n)&: \text{ the Lie algebra of all trace zero skew-Hermitian } n \times n \text{ martrices;} \\ SU(n)&: \text{ the Lie group of all special unitary } n \times n \text{ matrices;} \\ so(n,R)&: \text{ the Lie algebra of all } n \times n \text{ real skew-symmetric matrices;} \\ SO(n,R)&: \text{ the special orthogonal (Lie) group of } n \times n \text{ matrices;} \\ sp(2n,R)&: \text{ the symplectic Lie algebra} \\ &\equiv \left\{ X \in M(2n,\mathbb{R}) \;\middle|\; X^T J_{2n} = -J_{2n} X, J_{2n} = \begin{bmatrix} O_n & I_n \\ -I_n & O_n \end{bmatrix} \right\}; \\ so(p,q,\mathbb{R} \text{ or } \mathbb{C}) &= \left\{ X \in M(p+q, \mathbb{R} \text{ or } \mathbb{C}) \;\middle|\; X^T I_{p,q} = -I_{p,q} X, \right. \\ &\qquad \left. \text{with } I_{p,q} \equiv \begin{bmatrix} I_p & O_{p\times q} \\ O_{q\times p} & -I_q \end{bmatrix} \right\}. \end{aligned}$$

(In the above, $M(k, \mathbb{R} \text{ or } \mathbb{C})$ denotes the vector space of all $k \times k$ matrices over $\mathbb{R}$ or $\mathbb{C}$, $O_{p\times q}$ and $O_{q\times p}$ are zero matrices, and I_k denotes the $k \times k$ identity matrix.)□

EXAMPLE 3.2 (The Killing form). For a general Lie algebra $\mathfrak{g}$ and $X \in \mathfrak{g}$, first define

$$ad_X :\ \mathfrak{g} \to \mathfrak{g}, ad_X(Y) = [X, Y], \text{ for any } Y \in \mathfrak{g}.$$

Then the Killing form is defined by

$$\langle X, Y \rangle = \mathrm{Tr}(ad_X ad_Y) \qquad (\text{Tr: the trace operator}).$$

In the particular case $\mathfrak{g} = su(2)$, we can use the Pauli matrices as basis to calculate $\langle X, Y\rangle$ explicitly as follows: for $X, Y \in su(2)$,

$$X = a_1\frac{i\sigma_x}{2} + b_1\frac{i\sigma_y}{2} + c_1\frac{i\sigma_z}{2},$$
$$Y = a_2\frac{i\sigma_x}{2} + b_2\frac{i\sigma_y}{2} + c_2\frac{i\sigma_z}{2},$$

we have

$$\langle X, Y\rangle = -2(a_1a_2 + b_1b_2 + c_1c_2).$$

In other words, the Killing form is, up to a negative constant factor, the usual inner product on R^3. Details are omitted. □

Though not needed, for the purposes at hand, a Cartan decomposition of the Lie algebra yields a matrix factorization of elements of the group, as follows:

THEOREM 3.1 (Preliminary Cartan PK decomposition). *Given a Cartan decomposition $\mathfrak{g} = \widetilde{K} \oplus \widetilde{P}$ of a semisimple Lie algebra $\mathfrak{g}$, let $G = e^{\mathfrak{g}}$ be the connected Lie group corresponding to $\mathfrak{g}$. Then every element $X \in G$ can be written as*

$$X = PK,$$

where

$$P = e^p \text{ with } p \in \widetilde{P}, \text{ and } K = e^k \text{ with } k \in \widetilde{K}. \tag{3.2}$$

□

The following is an example of a preliminary Cartan PK decomposition.

EXAMPLE 3.3. It is known that

$$su(n) = so(n, R) \oplus \mathcal{I} \equiv \widetilde{P} \oplus \widetilde{K}, \tag{3.3}$$

where

$\mathcal{I} \subseteq su(n)$ is the class of all purely imaginary traceless $n \times n$ matrices.

So any $X \in SU(n)$ can be written as

$$X = PK$$

where P is the exponential of a skew-Hermitian purely imaginary matrix with trace zero, and K is a matrix in $SO(n, R)$. □

There is a refinement of the previous theorem, an ingredient of which is crucial for our purpose. To this end, we define the notion of a Cartan subalgebra relative to a Cartan decomposition. First, if there is a Lie subalgebra contained in $\widetilde{P}$, then it necessarily has to be abelian, since the direct sum condition implies $\widetilde{P} \cap \widetilde{K} = \{0\}$. We call any such *maximal* abelian subalgebra of $\widetilde{P}$ a *Cartan subalgebra* of the Cartan decomposition. The following intermediary result enables the refinement of Theorem 3.1.

THEOREM 3.2. *Let $\widetilde{A}$ be a Cartan subalgebra relative to the decomposition $\mathfrak{g} = \widetilde{K} \oplus \widetilde{P}$, Then*

$$\widetilde{P} = \bigcup_{K \in e^{\widetilde{K}}} K\widetilde{A}K^{-1}. \tag{3.4}$$

□

From this we have the following, which explains why Cartan decompositions are sometimes called KAK decompositions.

THEOREM 3.3 (Cartan KAK decomposition). *Let $\mathfrak{g}$ be a semisimple Lie algebra with a Cartan decomposition $\mathfrak{g} = \widetilde{K} \oplus \widetilde{P}$. Let $\widetilde{A}$ be a maximal subalgebra of $\mathfrak{g}$ such that $\widetilde{A} \subseteq \widetilde{P}$. Then every element of the Lie group $G = e^{\mathfrak{g}}$ can be written as*

$$X = K_1 A K_2,$$

where

$$K_j = e^{k_j} \text{ for } k_j \in \widetilde{K}, \text{ and } A = e^a \text{ for } a \in \widetilde{A}. \tag{3.5}$$

□

We now get to the core of the nuances of Cartan decompositions which are of relevance to us – namely, *their nonuniqueness*. There are two sources of nonuniqueness of Cartan decompositions of $su(n)$. First, given a *specific* Cartan decomposition, $su(n) = \widetilde{K} \oplus \widetilde{P}$, there are several possible Cartan subalgebras within $\widetilde{P}$ (and hence several decompositions of the type provided by Theorem 3.3). However, they are all conjugate. Specifically, we have the following.

THEOREM 3.4. *Given two Cartan subalgebras $\widetilde{A}_1$ and $\widetilde{A}_2$ in $\widetilde{P}$, there exists a $K = e^k$, $k \in \widetilde{K}$, such that*

$$K \widetilde{A}_1 K^{-1} = \widetilde{A}_2. \tag{3.6}$$

□

Since any two Cartan subalgebras are conjugate, they have identical dimensions, and this identical dimension is called the *rank* of the decomposition.

The second source of nonuniqueness is obtained by varying $\widetilde{K}$ and $\widetilde{P}$. Clearly, given an initial pair $\widetilde{K}$ and $\widetilde{P}$, we can obtain new Cartan decompositions by conjugating $\widetilde{K}$ and $\widetilde{P}$ by some (*but not all*) $Y \in SU(n)$. Such new Cartan decompositions are treated as equivalent. Specifically, we have the following definition.

DEFINITION 3.2. Two Cartan KAK decompositions

$$\mathfrak{g} = \widetilde{K}_1 \oplus \widetilde{P}_1, \text{ with } \widetilde{A}_1 \text{ being a Cartan subalgebra in } \widetilde{P}_1,$$
$$\mathfrak{g} = \widetilde{K}_2 \oplus \widetilde{P}_2, \text{ with } \widetilde{A}_2 \text{ being a Cartan subalgebra in } \widetilde{P}_2,$$

are said to be *equivalent* if there exists a $\mathcal{G} \in G = e^{\mathfrak{g}}$ such that

$$\mathcal{G}^\dagger \widetilde{K}_1 \mathcal{G} = \widetilde{K}_2, \quad \mathcal{G}^\dagger \widetilde{A}_1 \mathcal{G} = \widetilde{A}_2, \quad \mathcal{G}^\dagger \widetilde{P}_1 \mathcal{G} = \widetilde{P}_2. \tag{3.7}$$

□

Note that the above definition is often stated in the literature without the requirement that the corresponding Cartan subalgebras also be conjugate. However, upon invoking Theorem 3.4, in conjunction with the standard form of the above definition, one arrives at the version provided here.

We can now state the following.

THEOREM 3.5. *The Lie algebra $su(n)$ has exactly three types of non-equivalent decompositions labeled Types* I, II and III*, with* Type II *arising only if n is even.*□

For the purposes of this paper only Type **I** is relevant, and therefore we omit a detailed description of the other types. (Type I is explained below.) It is known that $\mathfrak{g} = su(4)$ has the following two KAK decompositions (all spans below are real linear spans):

(i)

$$\widetilde{K}_1 = \text{span}_{\mathbb{R}}\{i\sigma_j^{(1)} \otimes I_2^{(2)}, I_2^{(1)} \otimes i\sigma_k^{(2)} \mid j,k = x,y,z\}, \tag{3.8}$$

(with dimension 6);

$$\widetilde{P}_1 = \text{span}_{\mathbb{R}}\{i\sigma_j^{(1)} \otimes \sigma_k^{(2)} \mid j,k = x,y,z\}, \tag{3.9}$$

(with dimension 9);

$$\widetilde{A}_1 = \text{span}_{\mathbb{R}}\{i\sigma_j^{(1)} \otimes \sigma_j^{(2)} \mid j = x,y,z\}, \text{ a maximal Cartan subalgebra,} \tag{3.10}$$

(with dimension 3).

(ii)

$\widetilde{K}_2 = so(4,R)$, (with dimension 6);

$\widetilde{P}_2 = \mathcal{J}$ (the vector space of all purely imaginary traceless symmetric matrices in $su(4)$),

(with dimension 9)

$\widetilde{A}_2 =$ the (maximal) Cartan subalgebra of all purely imaginary *diagonal matrices* with trace 0.

(with dimension 3).

(iii) $\widetilde{K}_2, \widetilde{P}_2$ same as in item (ii), but with $\tilde{A}_2$ above being replaced by

$$\widetilde{A}_2' = \text{span}_{\mathbb{R}}\{i\sigma_x^{(1)} \otimes I^{(2)}, iI^{(1)} \otimes \sigma_x^{(2)}, i\sigma_x^{(1)} \otimes \sigma_x^{(2)}\}, \text{ a maximal Cartan subalgebra,} \tag{3.11}$$

(with dimension 3).

REMARK 3.1. Note that (ii), when stated for general n (not just $n = 4$) is the standard Type I decomposition, while (i) and (iii) are conjugate to the Type I decomposition.

The verification that the stated Cartan subalgebras are maximal is left to the reader. For instance, $\widetilde{A}_2$ is maximal, since there are diagonal matrices with distinct entries in $\widetilde{A}_2$, and hence any matrix commuting with such matrices has to be diagonal itself.

Now, by Theorem 3.5, there exist M, $M' \in SU(4)$ such that these two Type I Cartan decompositions are conjugate to each other, i.e.,

$$\begin{cases} M^\dagger \widetilde{K}_1 M = \widetilde{K}_2, & (3.12) \\ M^\dagger \widetilde{P}_1 M = \widetilde{P}_2, & (3.13) \\ M^\dagger \widetilde{A}_1 M = \widetilde{A}_2, & (3.14) \end{cases}$$

and

$$\begin{cases} M'^{\dagger}\widetilde{K}_2 M' = \widetilde{K}_2, & (3.15)\\ M'^{\dagger}\widetilde{P}_2 M' = \widetilde{P}_2, & (3.16)\\ M'^{\dagger}\widetilde{A}'_2 M = \widetilde{A}_2, & (3.17) \end{cases}$$

Since every element in $\widetilde{A}_2$ is a diagonal matrix, the above implies that the matrix M provides the conjugacy that simultaneously diagonalizes (all of) the matrices in $\widetilde{A}_1$. Now, of particular relevance to our problem is that iH_{QD} belongs to the Cartan subalgebra $\widetilde{A}_1$, while iH_{SQUID} belongs to the Cartan subalgebra $\widetilde{A}'_2$. Thus, the above matrices M and M' provide the unitary diagonalization we sought for.

We can now return to the devices in equation (2.8) and (2.12). (There is no need to examine H_{CQED} in (2.4) as we have noted in (2.16) that H_{CQED} is already in diagonal form.) We look at (2.10), the equivalent of (2.8), and immediately see that

$$iH_{\mathrm{QD}} \text{ (in (2.10))} = \omega[i\sigma_x^{(1)}\otimes\sigma_x^{(2)} + i\sigma_y^{(1)} + i\sigma_y^{(2)} + i\sigma_z^{(1)}\otimes\sigma_z^{(2)}] \in \widetilde{A}_1. \tag{3.18}$$

Therefore, we obtain the following.

THEOREM 3.6 (Diagonalization of H_{QD}). *For H_{QD} given by* (2.10)*, we have $iH_{QD} \in \widetilde{A}_1$ and, therefore, there exists an $M \in SU(4)$ such that*

$$M^{\dagger}H_{QD}M = \omega \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -3 \end{bmatrix} \tag{3.19}$$

is diagonalized. In particular, the magic basis matrix M:

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & i\\ 0 & i & 1 & 0\\ 0 & i & -1 & 0\\ 1 & 0 & 0 & i \end{bmatrix} \tag{3.20}$$

is one such matrix.

PROOF. The fact that $M^{\dagger}H_{\mathrm{QD}}M$ is diagonal follows from (3.14) because matrices in $\widetilde{A}_2$ are diagonal (with zero trace). The fact that the magic basis matrix M serves as the conjugacy is a well known fact in the quantum computing literature (cf. [**2, 3**], e.g.). See Miscellaneous comments (below for more on this issue). □

Regarding H_{SQUID}, we have the following.

THEOREM 3.7 (Diagonalization of H_{SQUID}). *For H_{SQUID} given by* (2.13)*, we have $iH_{SQUID} \in \widetilde{A}'_1$ and, therefore, there exists an $M' \in SU(4)$ such that*

$$M'^{\dagger}H_{SQUID}M' = \delta \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -3 \end{bmatrix}, \tag{3.21}$$

where the RHS is a diagonal matrix. In particular, we can choose

$$M' = V^{(1)}\otimes V^{(2)}, \text{ where } V^{(j)} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1\\ -1 & 1 \end{bmatrix} \text{ for } j = 1, 2.$$

PROOF. The diagonalization (3.21) easily follows from (3.17) and the fact that $iH_{\text{SQUID}} \in \widetilde{A}_2'$. Since the corresponding $\widetilde{K}$ and $\widetilde{P}$ are the same for the two Cartan decompositions in question, and only the Cartan subalgebras differ, it follows from Theorem 3.4 that there is a 4×4 special orthogonal matrix which renders these two subalgebras conjugate, and which, therefore, diagonalizes H_{SQUID}. Thus, in particular, a *real* matrix will achieve the conjugation (since special orthogonal matrices are real). Of course, this special orthogonal matrix renders the two Cartan decompositions of $su(4)$ conjugate as well.

In this case this conjugation can be found by inspection. Indeed, if we can find a 2×2 (real) special orthogonal matrix V such that $V^\dagger \sigma_x V$ is diagonal, then $V \otimes V$ will diagonalize H_{SQUID}. (This can be found more systematically using quaternions (which is omitted) and, once again, no eigenvector calculations are needed. The V in the statement of the theorem is but one such conjugating matrix.) □

Since the matrix M' satisfies $M'^\dagger \widetilde{A}_2' M' = \widetilde{A}_2$, we see that it would also diagonalize the initial form of the Hamiltonian of the SQUID, i.e., the Hamiltonian $H = -E_J^{(1)} \sigma_x^{(1)} \otimes I^{(2)} - E_J^{(2)} I^{(1)} \otimes \sigma_x^{(2)} + \Pi_{12} \sigma_x^{(1)} \otimes \sigma_x^{(2)}$.

Miscellaneous comments. The fact that the magic matrix conjugates the two Cartan decompositions in the proof of Theorem (3.6) has been known for some time. Indeed, the columns of M are maximally entangled two qubit states. Therefore, the effect of a local unitary matrix, $U \otimes V, U, V \in SU(2)$ is of natural interest. Denoting by $SU(2) \otimes SU(2)$ two qubit local unitaries, it was therefore soon established that $M^\dagger (SU(2) \otimes SU(2)) M = SO(4, R)$. Since $\widetilde{K}_1$ and $\widetilde{K}_2$ are precisely the Lie algebras of $SU(2) \otimes SU(2)$ and $SO(4, R)$, it follows that M conjugates these two Lie algebras also. From here it is just a little extra work to check that M conjugates the two associated Cartan decompositions also (including the associated Cartan subalgebras). So it is a natural question to inquire whether in absence of this history if one would have been able to arrive at M. The answer to this is a guarded yes. To that end we need a brief detour through the theory of Cartan involutions. A Cartan involution is a linear map $\Theta \colon \mathfrak{g} \to \mathfrak{g}$, which is in addition i) A Lie algebra homomorphism, and ii) an involution (i.e., $\Theta \circ \Theta = I$.) There is a close relationship between Cartan involutions and (preliminary) decompositions. For our purposes it suffices to explain this in the context to Type I decompositions of $su(n)$. Denote by $\widetilde{K}$ the $+1$-eigenspace of Θ, and by $\widetilde{P}$ the -1-eigenspace of Θ. Then it is routine to check that $\widetilde{K}, \widetilde{P}$ provide a preliminary Cartan decomposition of $su(n)$. The converse is true as well, i.e., every Cartan decomposition arises in the above manner from some Cartan involution. If one knows *explicitly* the Cartan involutions associated to a Cartan decomposition, then one can find the family of matrices which conjugate them.

Now the Cartan involution corresponding to standard Type I decomposition of $su(n)$ is $\Theta(X) = \overline{X}$, where $\overline{X}$ stands for complex (not Hermitian) conjugation, while it is known that the Cartan involution corresponding to any other Type I decomposition has to be given by $S\overline{X}S^\dagger$, with $S \in SU(n)$. Not every $S \in SU(n)$ is admissible, since $S\overline{X}S^\dagger$ will typically not be an involution. Once, after allowing for the above restriction, one has found the S corresponding to a given Type I Cartan decomposition it is possible to write algebraic conditions on the matrix (or matrices) M which will render the corresponding Cartan decomposition conjugate to the standard Type I Cartan decomposition. In the case of $su(4)$ and the pair

$(\widetilde{K}_1, \widetilde{P}_1)$, it turns out that $S = J_2 \otimes J_2$ (see [**3**]). Here

$$J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Hence one finds ([**3**]) that the most general $M \in SU(4)$ which conjugates the pairs $(\widetilde{K}_1, \widetilde{P}_1)$ and $(\widetilde{K}_2, \widetilde{P}_2)$ has to satisfy

$$MM^T = \zeta J_2 \otimes J_2, \tag{3.22}$$

where $\zeta^4 = 1$. One can systematically solve the last equation to see, in particular, that the magic matrix conjugates the pair $(\widetilde{K}_1, \widetilde{P}_1)$ and $(\widetilde{K}_2, \widetilde{P}_2)$. It is then easily checked that it also conjugates the corresponding Cartan subalgebras as well. Furthermore, it is seen from here that the most general matrix in $SU(4)$ which conjugates both Cartan decompositions (including the Cartan subalgebras) has to be of the form MD, where D is permutation equivalent to a real, special orthogonal diagonal matrix. Indeed, if M is the magic basis matrix and $\widetilde{M}$ a matrix in $SU(4)$ satisfying Equation (3.22), then $\widetilde{M} = MP$ for a matrix in $P \in SO(4, \mathbb{R})$. Since M already conjugates $\widetilde{A}_i$, it means that P is a special orthogonal matrix which takes all purely imaginary diagonal matrices to themselves, and hence it itself must be diagonal or permutation equivalent to it and thus $P = D \in SO(4, \mathbb{R})$.

In general Lie theoretic decompositions (such as Cartan or Iwasawa decompositions) do not supersede linear algebraic tools, but complement them in problems such as diagonalization. In some situations, as is the case with the problems considered here, one is able to invoke them to save the arduous (or perhaps even otherwise impossible) task and achieve simultaneous diagonalization in *closed* form, without requiring any eigenvector information. □

Conclusions

In this paper, we presented a unified treatment for universal 2-bit entangling operations by three different types of important physical systems. We were able to find explicitly conjugations up to phase between them. The key to this were two facts: i) Though the Hamiltonians describing them have different spectra, their eigenvalue multiplicity structures are identical; and ii) they each belong to the Cartan subalgebras of three different Type I Cartan decomposition of $su(4)$.

Though our interest, in this paper, was only in the universality of the Hamiltonians of these three devices for quantum computing, these explicit conjugations can, of course, be used for other purposes such as the control of these systems by external fields – results for one system will have immediate consequences for the others. Generalization of the ideas and methods to multi-qubit circuits is interesting and important but remains to be investigated.

References

[1] J.-L. Brylinski and R.K. Brylinski, Universal quantum gates, in *Mathematics of Quantum Computation*, R.K. Brylinski and G. Chen (eds.), Chapman & Hall/CRC, Boca Raton, Florida, 2002, 101–116.

[2] S.S. Bullock and G.K. Brennen, Canonical decomposition of n-qubit quantum computations and concurrence, quant-ph/0309104v3, 2/6/2004; *J. Math Phys.* **45** (2004), 2447–2467.

[3] S.S. Bullock, G.K. Brennen and D.P. O'Leary, Time reversal and n-qubit canonical decompositions, quant-ph/0402051v2, 12/22/2004; *J. Math. Phys.* **46** (2005), 062104.

[4] 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.
[5] G. Burkard, D. Loss and D.P. DiVincenzo, Coupled quantum dots as quantum gates, *Phys. Rev. B* **59** (1999), 2070–2078.
[6] D.P. DiVincenzo, Two-bit quantum gates are universal for quantum computation, *Phys. Rev. A* **51** (1995), 1015–1022.
[7] S. Helgason, *Differential Geometry and Symmetric Spaces*, AMS Chelsea Publishing, 2nd edition, American Mathematical Society, Providence, RI, 2001.
[8] P. Zanardi, C. Zalka and L. Faoro, Entangling power of quantum evolutions, *Phys. Rev. A* **62** (2000), 030301.
[9] Z. Zhang, V. Ramakrishna and G. Chen, Quantum computing devices, a short introduction, in *MHQP (Mathematical Horizons on Quantum Physics)*, Institute of Mathematical Sciences (IMS), National University of Singapore, IMS Lecture Notes Series, Vol. 20, World Scientific, Singapore, 2010.

Department of Mathematics and Institute for Quantum Science and Engineering, Texas A&M University, College Station, TX 77843

Department of Mathematics and Taida Institute for Mathematical Science (TIMS), National Taiwan University, Taipei, Taiwan, R.O.C.
E-mail address: gchen@math.tamu.edu

Department of Mathematical Science, University of Texas-Dallas, Richardson, TX 75080

Department of Mathematics, University of Houston, Houston, TX 77004

Contemporary Mathematics
Volume **536**, 2011

Efficient algorithm for a quantum analogue of 2-SAT

Sergey Bravyi

Abstract. Complexity of a quantum analogue of the satisfiability problem is studied. Quantum k-SAT is a problem of verifying whether there exists a state $|\Psi\rangle$ of n qubits such that its k-qubit reduced density matrices have support on prescribed subspaces. We present a classical algorithm solving quantum 2-SAT in a polynomial time. It generalizes the well-known algorithm for the classical 2-SAT. Besides, we show that for any $k \geq 4$ quantum k-SAT is complete in the complexity class QMA with one-sided error.

1. Introduction

Quantum analogues of classical complexity classes have been studied extensively during the last several years. From the practical perspective the most interesting of them is BQP — a class of problems that can be solved on a quantum computer in a polynomial time with bounded error probability. Another relevant class is QMA — a quantum analogue of NP. By definition, a language L belongs to QMA if a membership $x \in L$ can be efficiently verified on a quantum computer having access to a witness quantum state $|\psi_x\rangle$ playing the same role as a witness bit string in the definition of NP, see [**1**]. It is widely believed that QMA is strictly larger than NP.

There are only a few natural problems known to be QMA-complete. The results of the present paper concern the problem 2-local Hamiltonian introduced by Kitaev, see [**2, 1**]. It is a suitably formalized version of a fundamental problem in the quantum many-body physics: evaluate the ground state energy of n-qubit Hamiltonian which can be represented a sum of two-qubit interactions, $H = -\sum_{a<b} H_{a,b}$.

A theorem proven by Kitaev, Kempe, and Regev at [**2**] asserts that the problem 2-local Hamiltonian is QMA-complete. One way to interpret this result is to identify a classical analogue of the 2-local Hamiltonian problem. If one assumes that all interactions $H_{a,b}$ are diagonal in the standard $|0\rangle, |1\rangle$ basis of n qubits and that their eigenvalues may be either 0 or 1, the 2-local Hamiltonian problem becomes equivalent to MAX-2-SAT [**2**]. Indeed, in this case a ground state of H can be chosen as a basis vector $|x\rangle$ corresponding to some n-bit string x. An eigenvalue of $H_{a,b}$ on $|x\rangle$ is a Boolean function of bits x_a, x_b that can be represented as a conjuction of clauses $x_a \vee x_b$, $(\neg x_a) \vee x_b$, $x_a \vee (\neg x_b)$, $(\neg x_a) \vee (\neg x_b)$ (non-trivial

1991 *Mathematics Subject Classification.* 68Q12,11Y16,03D15.

Key words and phrases. Quantum complexity classes, local Hamiltonians, satisfiability problem.

interactions involve one, two, or three clauses). Accordingly, one can replace H by a list of 2-bit clauses, while the ground state energy of H is equal to the maximum number of clauses that can be satisfied simultaneously.

This quantum-to-classical mapping allows one to attribute QMA-completeness of the 2-local Hamiltonian problem to NP-completeness of MAX-2-SAT. On the other hand, classical problem 2-SAT (verify that *all* 2-bit clauses in a given list can be satisfied simultaneously) can be solved in a linear time [**3**], see also Appendix B. It rises the following natural questions:

- What is a quantum analogue of 2-SAT ?
- Does there exist a poly-time algorithm (classical or quantum) solving quantum 2-SAT ?

To define quantum 2-SAT we shall substitute a 2-bit clause $C_{a,b}$ involving some particular pair of bits x_a, x_b (for example, $C_{a,b} = x_a \vee (\neg x_b)$) by a pure two qubit state $|\phi_{a,b}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$. Quantum analogue of a property "n-bit string x satisfies the clause $C_{a,b}$" is a property "quantum state $|\Psi\rangle$ of n qubits has reduced density matrix $\rho_{a,b}$ orthogonal to $|\phi_{a,b}\rangle$". The latter means precisely that $\langle\phi_{a,b}|\rho_{a,b}|\phi_{a,b}\rangle = 0$, where $\rho_{a,b} = \mathrm{Tr}_{c\neq a,b}|\Psi\rangle\langle\Psi|$. Such a generalization seems justified since a two-bit clause $C_{a,b}$ is *not* satisfied only for one configuration of variables x_a, x_b (in the example above $x_a = 0$ and $x_b = 1$), so a satisfying assignment x must be orthogonal to this configuration. In general, there might be several clauses involving a pair of bits a, b. The corresponding two-qubit states $|\phi_{a,b}\rangle$ span a *forbidden subspace* $\mathcal{M}_{a,b} \subseteq \mathbb{C}^2 \otimes \mathbb{C}^2$, and a satisfying assignment $|\Psi\rangle$ must satisfy $\langle\phi|\rho_{a,b}|\phi\rangle = 0$ for any $|\phi\rangle \in \mathcal{M}_{a,b}$. Denoting $\Pi_{a,b}$ an orthogonal projector onto $\mathcal{M}_{a,b}$ multiplied by the identity operator on all other qubits, we obtain an equivalent condition $\Pi_{a,b}|\Psi\rangle = 0$. Thus quantum 2-SAT can be defined as follows:

Input: *An integer n and a family of 2-qubit projectors $\{\Pi_{a,b}\}$, $1 \le a < b \le n$.*
Problem: *Decide whether there exists a state $|\Psi\rangle$ of n qubits such that $\Pi_{a,b}|\Psi\rangle = 0$ for all $1 \le a < b \le n$.*

Note that there is no loss of generality in imposing constraints for every pair of qubits, since some of the projectors $\Pi_{a,b}$ may be equal to zero.

The main conclusion drawn in the present paper is that quantum 2-SAT is not harder than its classical counterpart. An efficient algorithm for quantum 2-SAT is described in Section 2. The key ingredient of the algorithm is Lemma 1 that allows one to generate new 2-qubit constraints from existing ones according to simple local rules. It can be illustrated by the following simple example. Suppose a state $|\Psi\rangle$ satisfies constraints $\Pi_{1,2}|\Psi\rangle = \Pi_{2,3}|\Psi\rangle = 0$, where $\Pi_{1,2} = |\Psi^-\rangle\langle\Psi^-|_{1,2} \otimes I_3$, and $\Pi_{2,3} = I_1 \otimes |\Psi^-\rangle\langle\Psi^-|_{2,3}$ are projectors onto the singlet state, $|\Psi^-\rangle = 2^{-1/2}(|0,1\rangle - |1,0\rangle)$. Taking into account that $I - \Pi_{1,2}$ and $I - \Pi_{2,3}$ are projectors onto the symmetric subspace of qubits $1, 2$ and $2, 3$ respectively, we conclude that $|\Psi\rangle$ is invariant under swaps of qubits $1 \leftrightarrow 2$ and $2 \leftrightarrow 3$. Thus $|\Psi\rangle$ is also invariant under a swap $1 \leftrightarrow 3$. Therefore we can generate a new constraint $\Pi_{1,3}|\Psi\rangle = 0$, where $\Pi_{1,3} = |\Psi^-\rangle\langle\Psi^-|_{1,3} \otimes I_2$. Lemma 1 generalizes this observation to projectors onto arbitrary two-qubit states (not necessarily entangled).

The algorithm is defined inductively, such that it allows one to reduce n-qubit 2-SAT to $(n-1)$-qubit 2-SAT in a polynomial time. Each step of the induction proceeds as follows (for a detailed analysis see Section 2). For each pair $1 \le a <$

$b \leq n$ we look at the rank $r_{a,b}$ of the projector $\Pi_{a,b}$ (the dimension of the forbidden subspace $\mathcal{M}_{a,b}$). If $r_{a,b} = 4$, the problem has no satisfying assignments. If $r_{a,b} = 3$, a state of qubits a, b is completely specified by a constraint $\Pi_{a,b} |\Psi\rangle = 0$ alone, so one can exclude them from consideration reducing n to $n-2$. If $r_{a,b} = 2$, qubits a and b can be merged into a single logical qubit supported on the zero subspace of $\Pi_{a,b}$. It reduces n to $n-1$. If $r_{a,b} \leq 1$ for all a and b, we invoke Lemma 1 to generate new constraints. The process of generating new constraints terminates whenever $r_{a,b} \geq 2$ is encountered at some pair of qubits (which reduces the total number of qubits), or if we arrive to what we call *a complete set of constraints*. We prove then that any instance with a complete set of constraints has a satisfying assignment (moreover, it can be chosen as a product of one-qubit states). The running time of the whole algorithm is $O(n^4)$.

A satisfiability problem in which clauses involve k bits is known as k-SAT. Quantum analogue of k-SAT can be specified by a family of k-qubit projectors $\{\Pi_S\}$, where $S \subseteq \{1, \ldots, n\}$ runs over all subsets of cardinality k. One needs to verify whether there exists an n-qubit state $|\Psi\rangle$ such that $\Pi_S |\Psi\rangle = 0$ for all S. Since k-SAT is known to be NP-complete for $k \geq 3$, one can ask whether quantum k-SAT is QMA-complete for $k \geq 3$? Before addressing this question it should be noted that the definition of quantum k-SAT given above is not quite satisfactory. Indeed, there might exist instances which have no exact satisfying assignments, meanwhile having an approximate solutions $|\Psi\rangle$ such that equations $\Pi_S |\Psi\rangle = 0$ are satisfied with an exponentially small error. To exclude such cases from consideration we shall introduce a precision parameter ϵ, $\epsilon \geq 1/n^\alpha$, $\alpha = O(1)$, separating positive and negative instances. The definition of quantum k-SAT given above must be complimented as follows:

Input: *An integer n, a real number $\epsilon = \Omega(1/n^\alpha)$, and a family of k-qubit projectors $\{\Pi_S\}$, $S \subseteq \{1, \ldots, n\}$, $|S| = k$.*
Promise: *Either there exists n-qubit state $|\Psi\rangle$ such that $\Pi_S |\Psi\rangle = 0$ for all S, or $\sum_S \langle\Psi|\Pi_S|\Psi\rangle \geq \epsilon$ for all $|\Psi\rangle$.*
Problem: *Decide which one is the case.*

To analyze complexity of quantum k-SAT we introduce a class QMA_1. It is defined in the same way as QMA with the only difference that for positive instances the verifying circuit accepts with probability one, see Section 3 for more details. The definition implies that $\mathrm{QMA}_1 \subseteq \mathrm{QMA}$.

We prove that quantum k-SAT with the promise as above is QMA_1-complete for $k \geq 4$. This result is quite unexpected since in general a subspace spanned by satisfying assignments of quantum k-SAT lacks a description in terms of l-qubit projectors for any $l < k$. So one could expect the complexity of quantum k-SAT to grow with k. Our result shows that this is not the case, at least for $k \geq 4$. Whether or not quantum 3-SAT is QMA_1-complete remains an open question.

The fact that quantum 5-SAT is QMA_1-complete easily follows from a possibility to represent the "computational history state" associated with a quantum circuit as a common zero vector of 5-qubit projectors, see [**1**]. A contribution reported in the present paper is essentially a reduction from $k = 5$ to $k = 4$. A mapping from a quantum circuit to a family of 4-qubit constraints that we use is

a significantly simplified version of a construction proposed in [**4**] (Section 4) for adiabatic quantum computation.

Remark: Input data for all problems discussed in the paper involve linear operators with complex matrix elements. To deal with exact equalities one has to use an appropriate exact representation of complex numbers. A good choice is algebraic numbers of bounded degree over the field of rational numbers (roots of polynomials with rational coefficients). All common linear algebra tasks for operators whose matrix elements are algebraic numbers can be solved efficiently, see books [**5, 6**] for the subject.

The rest of the paper is organized as follows. Efficient algorithm for quantum 2-SAT is presented in Section 2 (for the sake of completeness we outline the standard algorithm solving classical 2-SAT in Appendix B). QMA_1-completeness of quantum k-SAT, $k \geq 4$, is proved in Section 3. A technical lemma needed for this proof concerning universality of three-qubit quantum gates with matrix elements from a fixed field is placed in Appendix A.

2. Efficient algorithm for quantum 2-SAT

Let $\{\Pi_{a,b}\}$, $1 \leq a < b \leq n$ be an instance of quantum 2-SAT defined on n qubits. Without loss of generality $n \geq 3$. Obviously, these data can be encoded by a binary string x of length $O(n^2)$. We shall construct an algorithm that takes x as input and outputs one of the following

- Output 1: x has no satisfying assignments.
- Output 2: A list of one-qubit states $\{|\psi_j\rangle\}$ such that $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ is a satisfying assignment for x.
- Output 3: An instance y of quantum 2-SAT defined on $n-1$ or smaller number of qubits, such that y is equivalent to x.

The algorithm runs in a time $O(n^3)$. By applying it inductively $O(n)$ times one can reduce x to an equivalent instance involving a constant (say, $n = 2$) number of qubits which can be solved directly. It should be noted that although the algorithm allows one to construct one particular satisfying assignment (SA) for positive instances, this SA might not be a product of one-qubit states (the reduction corresponding to Output 3 may transform a product SA for y into entangled SA for x). Denote $r_{a,b}$ a rank of the projector $\Pi_{a,b}$. Without loss of generality $0 \leq r_{a,b} \leq 3$.

Definition 1. *An instance of quantum* 2*-SAT is called homogeneous iff* $r_{a,b} \leq 1$ *for all* a, b.

(Note that if $r_{a,b} = 0$, there is no any constraint for a pair of qubits a, b.) The first step of the algorithm is to verify whether x is homogeneous. If it is not, x can be transformed into an equivalent instance y on a smaller number of qubits (producing Output 3) as explained in Subsections A,B. If x is homogeneous (which is the most interesting case) one has to proceed to Subsection C.

2.1. Projectors of rank three. Suppose that $r_{a,b} = 3$ for some pair of qubits a, b, i.e.,

$$\Pi_{a,b} = I - |\phi\rangle\langle\phi|, \quad |\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2, \quad \langle\phi|\phi\rangle = 1.$$

An eigenvalue equation $\Pi_{a,b}|\Psi\rangle = 0$ implies that any SA has a product form $|\Psi\rangle = |\phi\rangle_{ab} \otimes |\Psi'\rangle$, where $|\Psi'\rangle$ is some state of the remaining $n-2$ qubits. Let us show

that $|\Psi\rangle$ is a SA iff $|\Psi'\rangle$ is a SA for a new instance y of quantum 2-SAT defined on $n-2$ qubits. Indeed, for any projectors P, Q one has

$$\left\{\begin{array}{rcl} P\,|\Psi\rangle &=& |\Psi\rangle, \\ Q\,|\Psi\rangle &=& |\Psi\rangle, \end{array}\right. \quad \text{iff} \quad \left\{\begin{array}{rcl} P\,|\Psi\rangle &=& |\Psi\rangle, \\ PQP\,|\Psi\rangle &=& |\Psi\rangle. \end{array}\right. \tag{1}$$

Let us choose any pair of qubits c, d and set

$$P = I - \Pi_{a,b} = |\phi\rangle\langle\phi|_{ab}, \quad Q = I - \Pi_{c,d}.$$

If the pairs (a, b) and (c, d) do not overlap, the right-hand side of Eq. (1) is equivalent to

$$|\Psi\rangle = |\phi\rangle_{ab} \otimes |\Psi'\rangle, \quad \Pi_{c,d}\,|\Psi'\rangle = 0.$$

On the other hand, if the pairs (a, b) and (c, d) overlap at one of the qubits, say $a = c$, then the right-hand side of Eq. (1) is equivalent to

$$|\Psi\rangle = |\phi\rangle_{ab} \otimes |\Psi'\rangle, \quad Q_d\,|\Psi'\rangle = |\Psi'\rangle,$$

where Q is a one-qubit self-adjoint operator implicitly defined by

$$|\phi\rangle\langle\phi|_{ab}\,(I - \Pi_{a,d})\,|\phi\rangle\langle\phi|_{ab} = |\phi\rangle\langle\phi|_{ab} \otimes Q_d.$$

Thus any 2-qubit constraint imposed on $|\Psi\rangle$ is equivalent to a 1-qubit or 2-qubit constraint imposed on $|\Psi'\rangle$. In other words, $|\Psi\rangle$ is a SA for x iff $|\Psi'\rangle$ is a SA for a new instance of quantum 2-SAT y defined on $n-2$ qubits.

2.2. Projectors of rank two. Suppose that $r_{a,b} = 2$ for some pair of qubits a, b. We shall argue that qubits a, b can be merged into a single logical qubit. It will yield a new instance y of quantum 2-SAT defined on $n-1$ qubits equivalent to x.

Indeed, let $V : \mathbb{C}^2 \to \mathbb{C}^2 \otimes \mathbb{C}^2$ be an isometry such that

$$\Pi_{a,b} = I - (VV^\dagger)_{ab}, \quad V^\dagger V = I.$$

The constraint $\Pi_{a,b}\,|\Psi\rangle = 0$ is equivalent to saying that

$$|\Psi\rangle = V_c\,|\Psi'\rangle,$$

where $|\Psi'\rangle$ is some $(n-1)$-qubit state and the label c refers to a qubit resulting from merging of a and b. The fact that V is an isometry implies that for any pair of qubits f, g

$$\Pi_{f,g}\,|\Psi\rangle = 0 \quad \text{iff} \quad V_c^\dagger\,\Pi_{f,g}\,V_c\,|\Psi'\rangle = 0. \tag{2}$$

If the pairs (a, b) and (f, g) do not overlap, the right-hand side of Eq. (2) is equivalent to $\Pi_{f,g}\,|\Psi'\rangle = 0$. On the other hand, if the pairs (a, b) and (f, g) overlap at one of the qubits, say $f = a$, then the right-hand side of Eq. (2) is equivalent to

$$Q_{c,g}\,|\Psi'\rangle = 0, \quad \text{where} \quad Q_{c,g} = V_c^\dagger\,\Pi_{a,g}\,V_c. \tag{3}$$

Obviously, $Q_{c,g}$ is a self-adjoint operator that acts only on two qubits c and g.

Thus any 2-qubit constraint imposed on $|\Psi\rangle$ is equivalent to a 2-qubit constraint imposed on $|\Psi'\rangle$. In other words, $|\Psi\rangle$ is a SA for x iff $|\Psi'\rangle$ is a SA for a new instance of quantum 2-SAT y defined on $n-1$ qubits.

2.3. Homogeneous 2-SAT. From now on we can assume that x is a homogeneous instance, i.e., all non-zero projectors have rank one. It will be convenient to describe a configuration of non-zero projectors by a graph $G=(V,E)$, such that $V=\{1,\ldots,n\}$, and $(a,b)\in E$ iff $\Pi_{a,b}\neq 0$. Now we can reformulate quantum 2-SAT as follows.
Input: A graph $G=(V,E)$ with n vertices and a list of rank two tensors $\phi^{(a,b)}$ assigned to edges $(a,b)\in E$.
Problem: Decide whether there exists a non-zero tensor ψ of rank n such that

$$\sum_{\alpha_a,\alpha_b} \phi^{(a,b)}_{\alpha_a,\alpha_b}\,\psi_{\alpha_1,\ldots,\alpha_n}=0 \quad \text{for any} \quad (a,b)\in E. \tag{4}$$

Comments: One should not confuse a rank of a tensor (number of its indexes) with a rank of a projector discussed in previous subsections. From now on we shall omit the summation symbol assuming that all repeated indexes are contracted. Indexes of all tensors take values 0 and 1. To avoid clutter in formulas, sometimes we shall identify tensors of rank two with 2×2 matrices and use matrix/vector multiplication. Let us also agree that $\phi^{(a,b)}_{\alpha,\beta}=\phi^{(b,a)}_{\beta,\alpha}$. We shall use a symbol ϵ for the fully antisymmetric tensor of rank two, i.e.,

$$\epsilon=\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}.$$

The following important observation provides a simple local rule for generating new constraints.

LEMMA 1. *Let ϕ, θ be arbitrary tensors of rank two and ψ be a tensor of rank three such that*

$$\phi_{\alpha,\beta}\,\psi_{\alpha,\beta,\gamma}=0 \quad \textit{and} \quad \theta_{\beta,\gamma}\,\psi_{\alpha,\beta,\gamma}=0.$$

Then ψ also obeys

$$\omega_{\alpha,\gamma}\,\psi_{\alpha,\beta,\gamma}=0, \quad \textit{where} \quad \omega_{\alpha,\gamma}=\phi_{\alpha,\beta}\,\epsilon_{\beta,\delta}\,\theta_{\delta,\gamma}.$$

Using matrix representation of rank two tensors, one has simply $\omega=\phi\,\epsilon\,\theta$.
Proof: Indeed,

$$\begin{aligned}\omega_{\alpha,\gamma}\,\psi_{\alpha,0,\gamma} &= \psi_{\alpha,0,\gamma}\,(\phi_{\alpha,0}\,\theta_{1,\gamma}-\phi_{\alpha,1}\theta_{0,\gamma})\\ &= -\psi_{\alpha,1,\gamma}\,\phi_{\alpha,1}\,\theta_{1,\gamma}-\psi_{\alpha,0,\gamma}\,\phi_{\alpha,1}\,\theta_{0,\gamma}\\ &= -\phi_{\alpha,1}\,(\psi_{\alpha,1,\gamma}\,\theta_{1,\gamma}+\psi_{\alpha,0,\gamma}\,\theta_{0,\gamma})=0.\end{aligned}$$

Analogously one proves that $\omega_{\alpha,\gamma}\,\psi_{\alpha,1,\gamma}=0$.

□

A straightforward generalization of the lemma is this. Suppose ψ is a tensor of rank n such that

$$\phi^{(a,b)}_{\alpha_a,\alpha_b}\,\psi_{\alpha_1,\ldots,\alpha_n}=0 \quad \text{and} \quad \phi^{(b,c)}_{\alpha_b,\alpha_c}\,\psi_{\alpha_1,\ldots,\alpha_n}=0 \tag{5}$$

for some tensors $\phi^{(a,b)}$ and $\phi^{(b,c)}$ of rank two and some integers $a\neq b\neq c$. Then ψ also obeys a constraint

$$\omega^{(a,c)}_{\alpha_a,\alpha_c}\,\psi_{\alpha_1,\ldots,\alpha_n}=0, \tag{6}$$

where

$$\omega^{(a,c)}_{\alpha,\gamma}=\phi^{(a,b)}_{\alpha,\beta}\,\epsilon_{\beta,\delta}\,\phi^{(b,c)}_{\delta,\gamma}. \tag{7}$$

Consider an instance x of 2-SAT specified by a graph $G = (V, E)$ and tensors $\phi^{(a,b)}$, $(a, b) \in E$. We can try to use Lemma 1 and its corollary Eqs. (6,7) to generate new constraints on ψ from the existing ones. Indeed, consider any pair of edges $(a, b) \in E$ and $(b, c) \in E$. Let $\omega^{(a,c)}$ be a tensor defined in Eq. (7). One has to consider the following possibilities:

(1) $\omega^{(a,c)} = 0$. We get no additional constraints on ψ.
(2) $\omega^{(a,c)} \neq 0$, but $(a, c) \in E$ and $\omega^{(a,c)}$ is proportional to $\phi^{(a,c)}$. Again, we get no additional constraints on ψ.
(3) $\omega^{(a,c)} \neq 0$ and $(a, c) \notin E$. In this case Eq. (6) provides a new constraint on ψ. Let us add (a, c) into the list of edges E and set $\phi^{(a,c)} = \omega^{(a,c)}$.
(4) $\omega^{(a,c)} \neq 0$, $(a, c) \in E$, and $\omega^{(a,c)}$ is not proportional to $\phi^{(a,c)}$. In this case we get two independent constraints for the pair of qubits a and c. They leave us with a two-dimensional forbidden subspace for this pair of qubits. Thus we can apply ideas of the previous subsection to merge a and c into a single logical qubit and obtain a new instance of quantum 2-SAT with $n - 1$ qubits which is equivalent to the original one.

Let us keep trying to generate new constraints by probing different pairs of edges until we either encounter the case 4 reducing the number of qubits from n to $n - 1$ (the algorithm terminates with Output 3), or after $O(n^3)$ steps we arrive to a homogeneous instance with *a complete set of constraints* which is defined below.

DEFINITION 2. *A graph $G = (V, E)$ and a family of rank two tensors $\phi^{(a,b)}$, $(a, b) \in E$ constitute a complete set of constraints iff for any pair of edges $(a, b) \in E$ and $(b, c) \in E$ one of the following is true*

- *If $(a, c) \in E$ then $\phi^{(a,b)} \epsilon \, \phi^{(b,c)}$ is either proportional to $\phi^{(a,c)}$ or zero,*
- *If $(a, c) \notin E$ then $\phi^{(a,b)} \epsilon \, \phi^{(b,c)} = 0$.*

This definition just says that any attempt to generate a new constraint on ψ using Lemma 1 would fail.

LEMMA 2. *Any homogeneous instance of quantum 2-SAT with a complete set of constraints has a satisfying assignment. It can be chosen as a product of one-qubit state.*

Remark: A proof given below is constructive. It allows one to find a product satisfying assignment in a time $O(n)$, $n = |V|$.

Proof: Let $\{\phi^{(a,b)}\}$, $(a, b) \in E$ be a family of rank two tensors constituting a complete set of constraints. We shall construct a satisfying assignment ψ which is a product of tensors of rank one:

$$\psi_{\alpha_1,\alpha_2,\ldots,\alpha_n} = \psi^{(1)}_{\alpha_1} \psi^{(2)}_{\alpha_2} \cdots \psi^{(n)}_{\alpha_n}.$$

Let us start from choosing an arbitrary $\psi^{(1)}$. Denote $\mathrm{nbgh}(a) \subset V$ a set of all nearest neighbors of a vertex a. The next step is to assign states to all vertices $a \in \mathrm{nbgh}(1)$ according to $\psi^{(a)} = \epsilon \, (\phi^{(1,a)})^T \, \psi^{(1)}$, or in tensor notations,

$$\psi^{(a)}_{\alpha} = \epsilon_{\alpha,\beta} \, \phi^{(1,a)}_{\gamma,\beta} \, \psi^{(1)}_{\gamma}, \quad a \in \mathrm{nbgh}(1)\,. \tag{8}$$

Let us verify that all constraints on edges incident to the vertex 1 are satisfied. Indeed,

$$\phi^{(1,a)}_{\delta,\alpha} \, \psi^{(1)}_{\delta} \, \psi^{(a)}_{\alpha} = \phi^{(1,a)}_{\delta,\alpha} \, \psi^{(1)}_{\delta} \, \epsilon_{\alpha,\beta} \, \phi^{(1,a)}_{\gamma,\beta} \, \psi^{(1)}_{\gamma} = 0$$

because ϵ is an antisymmetric tensor. This is equivalent to the desired constraints

$$\phi^{(1,a)}_{\alpha_1,\alpha_a}\,\psi_{\alpha_1,\ldots,\alpha_n}=0\quad\text{for any}\quad a\in\mathrm{nbgh}(1)\,.$$

The next step is to verify that all constraints on edges connecting two vertices from nbgh(1) are automatically satisfied. Indeed consider any pair of edges $(1,a)\in E$ and $(1,c)\in E$ such that $(a,c)\in E$ as well. Then by definition of a complete set of constraints we have $\phi^{(a,c)}=\phi^{(a,1)}\,\epsilon\,\phi^{(1,c)}$ (up to some overall factor). Since we have already fulfilled the constraints on the edges $(a,1)$ and $(1,c)$, we can apply Lemma 1 (with $b=1$) to infer that

$$\phi^{(a,c)}_{\alpha,\gamma}\,\psi^{(a)}_{\alpha}\,\psi^{(c)}_{\gamma}=0.$$

This is equivalent to the desired constraints

$$\phi^{(a,c)}_{\alpha_a,\alpha_c}\,\psi_{\alpha_1,\ldots,\alpha_n}=0\quad\text{for any}\quad a,c\in\mathrm{nbgh}(1),\quad(a,c)\in E.$$

Let us split the set of all vertices V into two subsets, $V=V_{close}\cup V_{far}$, where V_{close} consists of the vertex 1 and its nearest neighbors, while V_{far} consists of all other vertices (those having distance two or greater from the vertex 1). All vertices in V_{close} have been already assigned a state. This assignment satisfies the constraints on all edges having both ends in V_{close}. We shall now prove that this assignment also satisfies the constraints on any edge having one end in V_{close} and another end in V_{far}, for *any* choice of assignments in V_{far}.

Indeed, consider any edge $(b,c)\in E$, such that $b\in\mathrm{nbgh}(1)$ and $c\in V_{far}$. Since $(1,c)\notin E$, by definition of a complete set of constraints we have

$$\phi^{(1,b)}\,\epsilon\,\phi^{(b,c)}=0. \tag{9}$$

Let us verify that the constraint on the edge (b,c) is fulfilled for *all* choices of an assignment $\psi^{(c)}$, i.e.,

$$\phi^{(b,c)}_{\beta,\gamma}\,\psi^{(b)}_{\beta}\,\psi^{(c)}_{\gamma}=0\quad\text{for all}\quad\psi^{(c)}. \tag{10}$$

It suffices to verify that

$$\phi^{(b,c)}_{\beta,\gamma}\,\psi^{(b)}_{\beta}=0. \tag{11}$$

Indeed, from Eq. (8) we have

$$\psi^{(b)}_{\beta}=\epsilon_{\beta,\alpha}\,\phi^{(1,b)}_{\delta,\alpha}\,\psi^{(1)}_{\delta}.$$

Therefore

$$\phi^{(b,c)}_{\beta,\gamma}\,\psi^{(b)}_{\beta}=\phi^{(b,c)}_{\beta,\gamma}\,\epsilon_{\beta,\alpha}\,\phi^{(1,b)}_{\delta,\alpha}\,\psi^{(1)}_{\delta}=-(\phi^{(1,b)}\,\epsilon\,\phi^{(b,c)})_{\delta,\gamma}\,\psi^{(1)}_{\delta}=0,$$

see Eq. (9). Thus we have proved Eq. (11), and therefore Eq. (10). This is equivalent to the desired constraints

$$\phi^{(b,c)}_{\alpha_b,\alpha_c}\,\psi_{\alpha_1,\ldots,\alpha_n}=0\quad\text{for any}\quad b\in\mathrm{nbgh}(1),\quad c\in V_{far}. \tag{12}$$

for any choice of an assignment at the vertices $c\in V_{far}$.

The only constraints that we have not verified yet are those sitting on edges having both ends in V_{far}. One can easily check that a family of rank two tensors $\{\phi^{(a,b)}\}$, $a,b\in V_{far}$, $(a,b)\in E$, constitutes a complete set of constraints (since its definition is local). Thus we can keep applying the same algorithm to assign states to vertices from V_{far}. In this way we will finally end up with a SA for all n qubits.

□

3. Quantum 4-SAT is QMA_1 complete

Let us start from defining a complexity class QMA_1. Throughout this section all quantum circuits are assumed to have a data input register R_{in}, a witness input register R_{wit}, and an output register R_{out}. We shall assume that all qubits of the data input register R_{in} are set initially in $|0\rangle$ state. Final measurement involves measurement of each qubit from R_{out} in the standard $\{|0\rangle, |1\rangle\}$ basis. For any quantum circuit U and witness input state $|\psi_{wit}\rangle$ define an *acceptance probability* $AP(U, \psi_{wit})$ as a probability for the final measurement to yield the outcome 0 in every qubit of R_{out}.

Let $\mathcal{F} \subset \mathbb{C}$ be a field that we use for exact representation of complex numbers (see the remark in Introduction). We shall consider a gate set $\mathcal{G}$ consisting of all three-qubit unitary operators whose matrix elements in the standard basis belong to $\mathcal{F}$ (we include three-qubit gates into $\mathcal{G}$ just to simplify the proofs).

DEFINITION 3. *A language $L = L_{yes} \cup L_{no} \subset \Sigma^*$ belongs to QMA_1 iff there exists a polynomial p and uniform family of quantum circuits $\{U(x)\}$, $x \in L$, such that $U(x)$ has a length at most $p(|x|)$, $U(x)$ uses only gates from $\mathcal{G}$, $|R_{in}|+|R_{wit}|+|R_{out}| \leq p(|x|)$, and*

- *If $x \in L_{yes}$ then there exists a witness state $|\psi_{wit}\rangle$ such that $AP(U(x), \psi_{wit}) = 1$;*
- *If $x \in L_{no}$ then for any witness state $|\psi_{wit}\rangle$ one has $AP(U(x), \psi_{wit}) < 1 - 1/p(|x|)$.*

Since there is a polynomial gap between acceptance probabilities corresponding to positive and negative instances, we conclude that $\mathrm{QMA}_1 \subseteq \mathrm{QMA}$. From now on we shall assume that for any instance of quantum k-SAT projectors Π_S have matrix elements from the field $\mathcal{F}$.

LEMMA 3. *Quantum k-SAT belongs to QMA_1 for any constant k.*

Proof: Let $\{\Pi_S\}$, $S \subset \{1, 2, \ldots, n\}$, $|S| = k$ be an instance of quantum k-SAT. We shall construct a quantum circuit that measures eigenvalues of Π_S and writes the outcomes to output register R_{out}. More strictly, for each subset S, $|S| = k$, introduce an auxiliary qubit $q(S)$ initially prepared in the $|0\rangle$ state, and consider a unitary operator

$$U_S = \Pi_S \otimes \sigma^x_{q(S)} + (I - \Pi_S) \otimes I_{q(S)}.$$

It acts on a witness input register R_{wit} of size n and the auxiliary qubit $q(S)$. Note that U_S acts non-trivially only on a subset of $k+1$ qubits. According to Lemma 5, Appendix A, the operator U_S can be exactly represented by a quantum circuit of a size $poly(2^k)$ with gates from the set $\mathcal{G}$.

For any input witness state $|\psi_{wit}\rangle$ one has

$$U_S |\psi_{wit}\rangle \otimes |0\rangle = \Pi_S |\psi_{wit}\rangle \otimes |1\rangle + (I - \Pi_S) |\psi_{wit}\rangle \otimes |0\rangle. \tag{13}$$

Denote p_S a probability to measure the qubit $q(S)$ in the state $|1\rangle$ after the application of U_S. From Eq. (13) one can easily get

$$p_S = \langle \psi_{wit} | \Pi_S | \psi_{wit} \rangle.$$

Let us define the output register R_{out} as a collection of all ancillary qubits $q(S)$, one qubit for each subset S. Choose some order on the set of subsets S and define a verifying circuit as $U = \prod_S U_S$. By construction, U accepts on a witness state

$|\psi_{wit}\rangle$ iff all the qubits $q(S)$ have been measured in $|0\rangle$. A probability of that event can be bounded as

$$1-\sum_S p_S \le AP(U,\psi_{wit}) \le 1-\max_S p_S. \tag{14}$$

If there exists a satisfying assignment, one can choose $|\psi_{wit}\rangle$ such that $p_S=0$ for all S, and thus $AP(U,\psi_{wit})=1$. On the other hand, if there is no satisfying assignment, we are promised that for any witness state $\sum_S p_S \ge \epsilon$, where $\epsilon = 1/n^\alpha$, $\alpha = O(1)$, see Introduction. Therefore

$$\max_S p_S \ge \frac{\epsilon}{\binom{n}{k}} \ge n^{-k}\,\epsilon.$$

Combining it with Eq. (14) we get $AP(U,\psi_{wit}) \le 1-1/n^{k+\alpha}$ for any witness state $|\psi_{wit}\rangle$. Now one can easily choose a proper polynomial p to meet all the requirements of Definition 3.

□

LEMMA 4. *Quantum k-SAT is* QMA_1*-complete for any constant* $k \ge 4$.

Proof of Lemma 4: It suffices to prove that quantum 4-SAT is QMA_1-complete. Let $U = U_L \cdots U_2 U_1$, $U_j \in \mathcal{G}$, be a quantum circuit operating on N qubits with input data and witness registers R_{in} and R_{wit}, and output register R_{out}. Denote $|\psi_{in}\rangle = |0,\ldots,0\rangle$ and $|\psi_{wit}\rangle$ the initial states of R_{in} and R_{wit}. Without loss of generality we can assume that $N = |R_{in}| + |R_{wit}|$. The collection of N qubits $R_{in} \cup R_{wit}$ there the computation goes will be referred to as a *computational register*. It is described by a Hilbert space

$$\mathcal{H}_{\mathrm{comp}} = (\mathbb{C}^2)^{\otimes N}.$$

Let us define $L+1$ intermediate computational states

$$|Q_0\rangle = |\psi_{in}\rangle \otimes |\psi_{wit}\rangle \quad \text{and} \quad |Q_t\rangle = U_t\,|Q_{t-1}\rangle, \quad t=1,\ldots,L.$$

Introduce an auxiliary Hilbert space

$$\mathcal{H}_{\mathrm{clock}} = (\mathbb{C}^4)^{\otimes L}$$

that describes a *clock register* composed of L four-dimensional *clock particles*, one particle associated with each gate in the circuit. Each clock particle can be represented by a pair of qubits, so if we want to keep all projectors 4-local, we can afford only projectors acting on n_c clock particles and n_q computational qubits, where

$$(n_c, n_q) \in \{(2,0),\,(1,2),\,(0,4)\}.$$

Later on we shall define $2L$ orthonormal *legal clock states*

$$|C_1\rangle,\,|C_1'\rangle,\ldots,|C_L\rangle,\,|C_L'\rangle \in \mathcal{H}_{\mathrm{clock}}.$$

Our first goal is to design a Hamiltonian $H(U)$ such that

- $H(U)$ acts on a Hilbert space $\mathcal{H} = \mathcal{H}_{\mathrm{clock}} \otimes \mathcal{H}_{\mathrm{comp}}$,
- $H(U)$ is a sum of 4-qubit projectors;
- The zero-subspace of $H(U)$ is spanned by vectors

$$|\Omega(\psi_{wit})\rangle = \sum_{t=1}^{L} |C_t\rangle \otimes |Q_{t-1}\rangle + |C_t'\rangle \otimes |Q_t\rangle, \quad |Q_0\rangle = |\psi_{in}\rangle \otimes |\psi_{wit}\rangle. \tag{15}$$

The state $|\Omega(\psi_{wit})\rangle$ represents the whole history of the computation starting from a witness state $|\psi_{wit}\rangle$. Note that the gate U_t is applied when the clock register goes from the state $|C_t\rangle$ to the state $|C'_t\rangle$. On the other hand, as the clock register goes from $|C'_t\rangle$ to $|C_{t+1}\rangle$, the state of the computational register does not change.

Now let us specify the legal clock states. Basis states of a single clock particle will be denoted as $|u\rangle$ — *unborn*, $|d\rangle$ — *dead*, $|a1\rangle$ — *active phase 1*, $|a2\rangle$ — *active phase 2* (this terminology is partially borrowed from [**4**]. As the time goes forward, each clock particle evolves from the unborn phase to active phase 1, then to active phase 2 and finally ends up in the dead phase. Below we list the eight legal clock states for $L = 4$ as an example.

$$
\begin{array}{rclrcl}
|C_1\rangle &=& |a1,u,u,u\rangle, & |C_3\rangle &=& |d,d,a1,u\rangle,\\
|C'_1\rangle &=& |a2,u,u,u\rangle, & |C'_3\rangle &=& |d,d,a2,u\rangle,\\
|C_2\rangle &=& |d,a1,u,u\rangle, & |C_4\rangle &=& |d,d,d,a1\rangle,\\
|C'_2\rangle &=& |d,a2,u,u\rangle, & |C'_4\rangle &=& |d,d,d,a2\rangle.
\end{array}
\tag{16}
$$

In general, legal clock states are defined as basis vectors of $\mathcal{H}_{\rm clock}$ that obey the following constraints:

(1) The particle 1 is either active or dead,
(2) The particle L is either active or unborn,
(3) There is at most one active particle,
(4) If a particle j is dead for all $1 \le k < j$ a particle k is dead,
(5) If a particle j is unborn then for all $j < k \le L$ a particle k is unborn,
(6) If a particle j is dead then a particle $j+1$ is either dead or active.

One can easily check that there are only $2L$ basis states satisfying these rules. Each of these states has exactly one active particle (in either active phase 1 or active phase 2) at some position $1 \le j \le L$, dead particles at positions $k < j$ and unborn particles at positions $k > j$,

$$
|C_j\rangle = |\underbrace{d,\ldots,d}_{j-1},a1,\underbrace{u,\ldots,u}_{L-j}\rangle, \quad |C'_j\rangle = |\underbrace{d,\ldots,d}_{j-1},a2,\underbrace{u,\ldots,u}_{L-j}\rangle.
$$

Denote

$$
\mathcal{H}_{\rm legal} = \text{Linear Span}(|C_1\rangle,|C'_1\rangle,\ldots,|C_L\rangle,|C'_L\rangle) \subset \mathcal{H}_{\rm clock}
$$

a subspace spanned by the legal clock states. Let us define a Hamiltonian $H_{\rm clock}$ acting on the space $\mathcal{H}_{\rm clock}$ as

$$
H_{\rm clock} = \sum_{j=1}^{6} H^{(j)}_{\rm clock},
$$

$$
\begin{aligned}
H^{(1)}_{\rm clock} &= |u\rangle\langle u|_1, \\
H^{(2)}_{\rm clock} &= |d\rangle\langle d|_L, \\
H^{(3)}_{\rm clock} &= \sum_{1\le j<k\le L} (|a1\rangle\langle a1| + |a2\rangle\langle a2|)_j \otimes (|a1\rangle\langle a1| + |a2\rangle\langle a2|)_k, \\
H^{(4)}_{\rm clock} &= \sum_{1\le j<k\le L} (|a1\rangle\langle a1| + |a2\rangle\langle a2| + |u\rangle\langle u|)_j \otimes |d\rangle\langle d|_k, \\
H^{(5)}_{\rm clock} &= \sum_{1\le j<k\le L} |u\rangle\langle u|_j \otimes (|a1\rangle\langle a1| + |a2\rangle\langle a2| + |d\rangle\langle d|)_k, \\
H^{(6)}_{\rm clock} &= \sum_{1\le j\le L-1} |d\rangle\langle d|_j \otimes |u\rangle\langle u|_{j+1}.
\end{aligned}
$$

The six terms of $H_{\rm clock}$ correspond to the six constraints listed above, so that

$$|\psi\rangle \in \mathcal{H}_{\rm legal} \quad \text{iff} \quad H_{\rm clock}\,|\psi\rangle = 0. \tag{17}$$

Note that $H_{\rm clock}$ is a sum of 4-qubit projectors. Denote Π an orthogonal projector onto a subspace $\mathcal{H}_{\rm legal} \otimes \mathcal{H}_{\rm comp}$,

$$\Pi = \sum_{j=1}^{L} (|C_j\rangle\langle C_j| + |C'_j\rangle\langle C'_j|) \otimes I_{\rm comp}.$$

Define a Hamiltonian $H_{\rm init}$ as

$$H_{\rm init} = |a1\rangle\langle a1|_1 \otimes \left(\sum_{b\in R_{in}} |1\rangle\langle 1|_b \right). \tag{18}$$

The only legal clock state having $|a1\rangle$ in the first position is $|C_1\rangle$. Thus $H_{\rm init}$ penalizes any qubit of the input data register R_{in} for being in a state $|1\rangle$ provided that the clock register's state is $|C_1\rangle$. A restriction of $H_{\rm init}$ onto the subspace $\mathcal{H}_{\rm legal} \otimes \mathcal{H}_{\rm comp}$ is therefore

$$\Pi\, H_{\rm init}\, \Pi = |C_1\rangle\langle C_1| \otimes \left(\sum_{b\in R_{in}} |1\rangle\langle 1|_b \right). \tag{19}$$

Note that $H_{\rm init}$ is a sum of 3-qubit projectors.

Define a Hamiltonian $H_{\rm prop}$ as

$$H_{\rm prop} = \sum_{t=1}^{L} H_{{\rm prop},t} + \sum_{t=1}^{L-1} H'_{{\rm prop},t}, \tag{20}$$

where

$$H_{{\rm prop},t} = \frac{1}{2}\left[(|a1\rangle\langle a1| + |a2\rangle\langle a2|)_t \otimes I_{\rm comp} - |a2\rangle\langle a1|_t \otimes U_t - |a1\rangle\langle a2|_t \otimes U_t^\dagger \right], \tag{21}$$

and

$$H'_{{\rm prop},t} = \frac{1}{2}\left(|a2,u\rangle\langle a2,u| + |d,a1\rangle\langle d,a1| - |d,a1\rangle\langle a2,u| - |a2,u\rangle\langle d,a1| \right)_{t,t+1} \otimes I_{\rm comp}. \tag{22}$$

The operators $H_{{\rm prop},t}$ and $H'_{{\rm prop},t}$ are 4-qubit projectors. By inspecting the example Eq. (16) one can easily check that

- The only legal clock state having $a1$ at position t is $|C_t\rangle$;

- The only legal clock state having $a2$ at position t is $|C'_t\rangle$;
- The only legal clock state having $(d, a1)$ at positions $t, t+1$ is $|C_{t+1}\rangle$;
- The only legal clock state having $(a2, u)$ at positions $t, t+1$ is $|C'_t\rangle$.

Thus a restriction of $H_{prop,t}$ onto the subspace $\mathcal{H}_{legal} \otimes \mathcal{H}_{\rm comp}$ is

(23)
$$\Pi\, H_{prop,t}\, \Pi = \frac{1}{2}\left[(|C_t\rangle\langle C_t| + |C'_t\rangle\langle C'_t|) \otimes I_{\rm comp} - |C'_t\rangle\langle C_t| \otimes U_t - |C_t\rangle\langle C'_t| \otimes U_t^\dagger\right].$$

Analogously, a restriction of $H'_{prop,t}$ onto the subspace $\mathcal{H}_{legal} \otimes \mathcal{H}_{\rm comp}$ is

$$\Pi\, H'_{prop,t}\, \Pi = \frac{1}{2}\left(|C'_t\rangle\langle C'_t| + |C_{t+1}\rangle\langle C_{t+1}| - |C_{t+1}\rangle\langle C'_t| - |C'_t\rangle\langle C_{t+1}|\right) \otimes I_{\rm comp}. \quad (24)$$

Define a Hamiltonian

$$H(U) = H_{\rm init} + H_{\rm clock} + H_{\rm prop}.$$

Combining Eqs. (19,23,24) one can easily check that the zero-subspace of $H(U)$ is indeed spanned by computational history states $|\Omega(\psi_{wit})\rangle$.

One remains to introduce an extra term into $H(U)$ that is responsible for the final measurement of R_{out}. Define

$$H_{\rm out} = |a2\rangle\langle a2|_L \otimes \left(\sum_{b \in R_{out}} |1\rangle\langle 1|_b\right).$$

The only legal clock state having $a2$ at the position L is $|C'_L\rangle$. Thus a restriction of $H_{\rm out}$ onto the subspace $\mathcal{H}_{\rm legal} \otimes \mathcal{H}_{\rm comp}$ is

$$\Pi\, H_{\rm out}\, \Pi = |C'_L\rangle\langle C'_L| \otimes \left(\sum_{b \in R_{out}} |1\rangle\langle 1|_b\right).$$

Therefore $H_{\rm out}$ penalizes any qubit of the output register for being in the state $|1\rangle$ provided that the clock register is in the state $|C'_L\rangle$. Besides, $H_{\rm out}$ is a sum of 3-qubit projectors.

We summarize that a Hamiltonian

$$H = H_{\rm init} + H_{\rm clock} + H_{\rm prop} + H_{out} \quad (25)$$

has zero ground state energy iff there exists input witness state $|\psi_{wit}\rangle$ such that $AP(U, \psi_{wit}) = 1$. By construction, H operates on $N + 2L$ qubits, and it can be represented as a sum of 4-qubit projectors:

$$H = \sum_S \Pi_S, \quad S \subseteq \{1, \ldots, N + 2L\}, \quad |S| = 4. \quad (26)$$

Thus the property "H has zero ground state energy" is equivalent to the quantum 4-SAT $\{\Pi_S\}$ having a satisfying assignment.

Let $L = L_{yes} \cup L_{no}$ be a language from QMA_1, $x \in L$ be a binary string, and $U(x)$ be a verifying circuit see Definition 3. Using the majority voting to amplify the gap in acceptance probabilities, see [**1**], we can assume that

- If $x \in L_{yes}$ then $AP(U, \psi_{wit}) = 1$ for some input witness state $|\psi_{wit}\rangle$,
- If $x \in L_{no}$ then $AP(U, \psi_{wit}) \leq \epsilon$, $\epsilon = 1/p(|x|)$, for all $|\psi_{wit}\rangle$,

where U is a circuit implementing several copies of $U(x)$ and the majority voting (obviously it can be realized using the gate set $\mathcal{G}$). The polynomial p above may be different from the one in Definition 3.

To complete the proof of the lemma we have to show that for negative instances, $x \in L_{no}$, the ground state energy of the Hamiltonian Eq. (25) is not too small, i.e., $\langle\Psi|H|\Psi\rangle \geq 1/q(|x|)$ for any $|\Psi\rangle$, where q is some polynomial. It can be done using ideas from [**1**]. Indeed, a decomposition

$$\mathcal{H} = \mathcal{H}_{\rm legal} \otimes \mathcal{H}_{\rm comp} \oplus \mathcal{H}_{\rm legal}^{\perp} \otimes \mathcal{H}_{\rm comp}$$

is invariant under H. Let H' be a restriction of H onto $\mathcal{H}_{\rm legal} \otimes \mathcal{H}_{\rm comp}$. One can easily check that H' is exactly the Hamiltonian that one would assign to a quantum circuit $\tilde{U}$ using the construction of [**1**], where $\tilde{U}$ is obtained from U by appending the identity gate to each gate of U (if U has a length L then $\tilde{U}$ has a length $2L$). It was shown in [**1**] that H' has the ground state energy at least $c(1-\sqrt{\epsilon})(2L)^{-3}$, where c is a constant and ϵ is defined above. It may be only polynomially small in $|x|$.

Let H'' be a restriction of H onto $\mathcal{H}_{\rm legal}^{\perp} \otimes \mathcal{H}_{\rm comp}$. Since any state from $\mathcal{H}_{\rm legal}^{\perp}$ violates at least one constraint from $H_{\rm clock}$, the ground state energy of H'' is at least 1.

□

Remark 1: One could also try to consider clock particles with only three states: unborn, active, and dead. It is possible to design a proper dynamics of the clock register, such that the computational history state can be specified by 3-local projectors [**7**]. Each projector involves a triple of particles with dimensions $3 \times 2 \times 2$.

Remark 2: If one modifies Definition 3 such that the acceptance probability corresponding to negative instances is $1-\epsilon$, where $\epsilon > 0$ may be arbitrarily small, the corresponding class would be hard for the polynomial hierarchy, as it would contain the exact counting class C$_=$P, see [**9**]. The same remark concerns quantum k-SAT, $k \geq 4$, without the polynomial gap promise.

Acknowledgements

The author would like to thank David DiVincenzo, Roberto Oliveira, and Barbara Terhal for numerous discussions and useful comments. Inspiring correspondence on quantum complexity classes with Mikhail Vyalyi is acknowledged. Part of this work was carried out when the author was a member of the Institute for Quantum Information, Caltech, supported by the National Science Foundation under grant number EIA-0086038.

References

[1] A. Kitaev, A. Shen, and M. Vyalyi *"Classical and quantum computation"*, Graduate Studies in Mathematics, Vol. **47**, American Mathematical Society (2002).

[2] J. Kempe, A. Kitaev, and O. Regev *"The complexity of the local Hamiltonian problem"*, quant-ph/0406180.

[3] B. Aspvall, M. Plass, and R. Tarjan *"A linear-time algorithm for testing the truth of certain quantified boolean formulas"*, Info. Proc. Letters, Vol. **8**, Iss. 3, p. 121-123 (1979).

[4] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev *"Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation"*, Proceedings of 45th FOCS (2004), quant-ph/0405098.

[5] A. Aho, J. Hopcroft, and J. Ullman *"The Design and Analysis of Computer Algorithms"*, Addison-Wesley Reading, Massachusetts (1974).

[6] D. Bini and V.Y. Pan *"Polynomial and matrix computation"*, Vol. **1**, Birkhäuser, Boston, Cambridge, MA (1994).

[7] David DiVincenzo, private communication.

[8] A. Barenco, C. H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, H. Weinfurter *"Elementary gates for quantum computation"*, Phys. Rev. **A52**, p. 3457 (1995).

[9] S. Fenner, F. Green, S. Homer, R. Pruim *"Determining Acceptance Possibility for a Quantum Computation is Hard for the Polynomial Hierarchy"*, quant-ph/9812056.

Appendix A. Quantum circuits over a fixed field

LEMMA 5. *Let V be a unitary operator acting on k qubits. Suppose that matrix elements of V in the standard basis belong to a field $\mathcal{F} \subset \mathbb{C}$. Then V can be exactly represented by a quantum circuit of size $poly(k) \cdot 2^{2k}$ with three-qubit gates whose matrix elements in the standard basis also belong to the field $\mathcal{F}$.*

Proof: The first step directly follows the proof of universality of two-qubit gates, see [**8**]. Let us decompose V as $V = \tilde{W}_1 \tilde{W}_2 \cdots \tilde{W}_L$, where each operator $\tilde{W}_j$ is a direct sum of 2x2 unitary on a two-dimensional subspace spanned by some pair of basis vectors and the identity operator on a subspace spanned by the remaining $2^k - 2$ basis vectors. Accordingly, $L = 2^{k-1}(2^k - 1)$ is the number of such subspaces. Matrix elements of the operators $\tilde{W}_j$ belong to the same field $\mathcal{F}$. Using swaps of qubits and σ^x gates one can transform any operator $\tilde{W}_j$ as above into a controlled one-qubit gate with one target qubit and $k-1$ control qubits, $\tilde{W}_j \equiv \Lambda_{k-1}(U_j)$. Here U_j is a one-qubit gate with matrix elements from $\mathcal{F}$.

Consider a classical unitary operator Ω that reversibly computes logical AND of k bits $x_1, \ldots, x_{k-1}$, i.e.,

$$\Omega \, |a\rangle \otimes |x_1, x_2, \ldots, x_{k-1}\rangle = |a \oplus AND(x_1, \ldots, x_{k-1})\rangle \otimes |x_1, x_2, \ldots, x_{k-1}\rangle.$$

Here $|a\rangle$ refers to an ancillary qubit. Since three-bit classical gates constitute universal basis for classical reversible computation, we can implement Ω (probably using additional $|0\rangle$ ancillas) by a circuit of size $poly(k)$ with three-qubit gates whose matrix elements are only 0 and 1. Now one can implement $\Lambda_{k-1}(U_j)$ as follows (we label the ancillary qubit by A and the target qubit by T):
(1) Set A to $|0\rangle$,
(2) Apply Ω to A and the $k-1$ control qubits,
(3) Apply $\Lambda(U_j)$ to A and T such that A is the control qubit,
(4) Apply Ω^{-1} to A and the $k-1$ control qubits.

One can easily check that the ancillary qubit ends up in the $|0\rangle$ state, while the $k-1$ control qubits and the target qubit are acted on by $\Lambda_{k-1}(U_j)$. By composing these circuits for each j one gets a circuit representing V.

□

Appendix B. Efficient algorithm for classical 2-SAT

Let $x = (x_1, \ldots, x_n)$ be a binary string. A Boolean function $l(x)$ is called a *literal* if $l(x) = x_a$ or $l(x) = (\neg x_a)$ for some $1 \le a \le n$. Given m Boolean functions (clauses) $C_j(x) = l_j(x) \vee l'_j(x)$, where l_j and l'_j are literals, a classical 2-SAT problem is to determine whether there exists a string x such that $C_j(x) = 1$ for all $j = 1, \ldots, m$. Below we briefly describe a well-known algorithm for a classical 2-SAT that runs in a time $O(n+m)$.

Without loss of generality $l'_j \neq (\neg l_j)$ (otherwise $C_j(x) = 1$ for all x). Consider a directed graph $G = (V, E)$, whose vertices are literals, i.e.,

$$V = \{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\},$$

and whose edges are pairs of literals (l, l') that appear in the same clause as shown below:

$$E = \{(l, l') \,:\, C_j = l \vee (\neg l') \quad \text{for some} \quad j\}.$$

Each clause C_j contributes to one or two edges of G. Let us split V into strongly connected components (SCC). (By definition, l and l' belong to the same SCC iff there exists a path from l to l' and a path from l' to l.) Obviously, one can identify all SCCs of G in a time $O(n+m)$.

LEMMA 6. *A satisfying assignment x exists iff for any $l \in V$ vertices l and $\neg l$ belong to different SCCs.*

Proof:
(a) Suppose for some $l, l' \in V$ there exists a path from l to l'. If x is a SA then $l(x) = 0$ implies $l'(x) = 0$. If l and $\neg l$ belong to the same SCC, then $l(x) = 0$ implies $\neg l(x) = 0$ and $\neg l(x) = 0$ implies $l(x) = 0$. This is a contradiction.
(b) Suppose that l and $\neg l$ belong to different SCCs for all $l \in V$. Let us find a SA. Consider a directed graph $\tilde{G} = (\tilde{V}, \tilde{E})$ whose vertices are SCCs of G and whose edges are pairs (S, S') of SCCs of G such that there exists a path from S to S'. By definition, $\tilde{G}$ is acyclic. Using the topological sorting algorithm one can order vertices of $\tilde{G}$ such that $(S, S') \in \tilde{E}$ implies $S < S'$. It can be done in a time $O(n+m)$.

By definition of G, for any vertices $l, l' \in V$ a path from l to l' and a path from $\neg l'$ to $\neg l$ exist or do not exist simultaneously. Thus for any vertex S of $\tilde{G}$ there exists a unique vertex $\neg S$ of $\tilde{G}$ such that $\neg S = \{l \in V \,:\, \neg l \in S\}$.

For all vertices S of $\tilde{G}$ do the following: If $S < (\neg S)$ then set $l = 1$ for all $l \in S$ and set $l = 0$ for all $l \in (\neg S)$. If $S > (\neg S)$ then set $l = 0$ for all $l \in S$ and set $l = 1$ for all $l \in (\neg S)$. We end up with some assignment x. Let us check that $C_j(x) = 1$ for all j. Indeed, otherwise we would have $l_j(x) = l'_j(x) = 0$ for some j. Let S and S' be SCCs of l_j and l'_j. We have $S > \neg S$ and $S' > \neg S'$. On the other hand, $S < \neg S'$ and $S' < \neg S$. This is a contradiction. Thus x is a SA.

□

IBM T.J. WATSON RESEARCH CENTER,, YORKTOWN HEIGHTS, NY 10598
E-mail address: sbravyi@us.ibm.com

Contemporary Mathematics
Volume **536**, 2011

Quantum Computational Curvature and Jacobi Fields

Howard E. Brandt

Abstract. Recent developments in the differential geometry of quantum computation are exposited. In the Riemannian geometry of quantum computation, the quantum evolution is described in terms of the special unitary group of n-qubit unitary operators with unit determinant. The group manifold is taken to be Riemannian. To elaborate on several aspects of the methodology on the group manifold, the Riemannian curvature, geodesic equation, Jacobi equation, generic lifted Jacobi equation, lifted Jacobi equation for varying penalty parameter, and the so-called geodesic derivative are reviewed. This is important for investigations of conjugate points and the global characteristics of geodesic paths in the group manifold, and the determination of optimal quantum circuits for carrying out a quantum computation.

1. INTRODUCTION

In the Riemannian geometry of quantum computation, a Riemannian metric can be chosen on the manifold of the (4^n-1)-dimensional Lie Group $SU(2^n)$ (special unitary group) of n-qubit unitary operators with unit determinant [**1**]-[**18**]. The traceless Hamiltonian of a quantum computational system is a tangent vector to a point on the group manifold of the n-qubit unitary transformation describing the time evolution of the system. The Hamiltonian H is an element of the Lie algebra $su(2^n)$ of traceless $2^n \times 2^n$ Hermitian matrices [**16**]-[**18**] and is tangent at the n-qubit unitary operator U to the evolutionary curve $e^{-iHt}U$ at $t = 0$. (Here and throughout, units are chosen such that Planck's constant divided by 2π is $\hbar = 1$.)

The Riemannian metric (inner product) $\langle ., . \rangle$ is a positive definite bilinear form $\langle H, J \rangle$ defined on tangent vectors (Hamiltonians) H and J. The n-qubit Hamiltonian H can be divided into two parts $P(H)$ and $Q(H)$, where $P(H)$ contains only

2000 *Mathematics Subject Classification.* Primary 81P68, 81-01, 81-02, 53B20, 53B50, 22E60, 22E70, 03D15, 53C22; Secondary 22D10, 43A75, 51N30, 20C35, 81R05.

Key words and phrases. quantum computing, quantum circuits, quantum complexity, unitary group, differential geometry, Riemannian geometry, curvature, geodesics, Lax equation, Jacobi fields.

The author wishes to thank Kazem Mahdavi for the invitation to present this paper at the National Science Foundation sponsored conference on Representation Theory, Quantum Field Theory, Mathematical Physics and Quantum Information Theory held at the University of Texas at Tyler, 1-4 October 2009.

This research was supported by the Director's Research Initiative of the U.S. Army Research Laboratory.

one and two-body terms, and $Q(H)$ contains more than two-body terms [**1**]. Thus:

$$H = P(H) + Q(H), \tag{1.1}$$

in which P and Q are superoperators acting on H, and obey the following relations:

$$P + Q = I, \quad PQ = QP = 0, \quad P^2 = P, \quad Q^2 = Q, \tag{1.2}$$

where I is the identity.

The Hamiltonian can be expressed in terms of tensor products of the Pauli matrices. The Pauli matrices are given by [**19**]

$$\begin{aligned} &\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \ \sigma_1 \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ &\sigma_2 \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \ \sigma_3 \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned} \tag{1.3}$$

They are Hermitian,

$$\sigma_i = \sigma_i^\dagger \ , i = 0, 1, 2, 3, \tag{1.4}$$

where † denotes the adjoint, and, except for σ_0, they are traceless,

$$\mathrm{Tr}\sigma_i = 0, \quad i \neq 0. \tag{1.5}$$

Their products are given by

$$\sigma_i^2 = I. \tag{1.6}$$

Also,

$$\sigma_i \sigma_j = i\varepsilon_{ijk}\sigma_k, \quad i, j, k \neq 0, \tag{1.7}$$

expressed in terms of the totally antisymmetric Levi-Civita symbol with $\varepsilon_{123} = 1$, and using the Einstein sum convention.

An example of Eq. (1.1), in the case of a 3-qubit Hamiltonian, is

$$\begin{aligned}
P(H) = {} & x_1\sigma_1\otimes I\otimes I \\
& + x_2\sigma_2\otimes I\otimes I + x_3\sigma_3\otimes I\otimes I \\
& + \ x_4 I\otimes\sigma_1\otimes I + x_5 I\otimes\sigma_2\otimes I \\
& + x_6 I\otimes\sigma_3\otimes I + \ x_7 I\otimes I\otimes\sigma_1 \\
& + x_8 I\otimes I\otimes\sigma_2 + x_9 I\otimes I\otimes\sigma_3 \\
& + \ x_{10}\sigma_1\otimes\sigma_2\otimes I + x_{11}\sigma_1\otimes I\otimes\sigma_2 \\
& + x_{12} I\otimes\sigma_1\otimes\sigma_2 + \ x_{13}\sigma_2\otimes\sigma_1\otimes I \\
& + x_{14}\sigma_2\otimes I\otimes\sigma_1 + x_{15} I\otimes\sigma_2\otimes\sigma_1 \\
& + \ x_{16}\sigma_1\otimes\sigma_3\otimes I + x_{17}\sigma_1\otimes I\otimes\sigma_3 \\
& + x_{18} I\otimes\sigma_1\otimes\sigma_3 + \ x_{19}\sigma_3\otimes\sigma_1\otimes I \\
& + x_{20}\sigma_3\otimes I\otimes\sigma_1 + x_{21} I\otimes\sigma_3\otimes\sigma_1 \\
& + \ x_{22}\sigma_2\otimes\sigma_3\otimes I + x_{23}\sigma_2\otimes I\otimes\sigma_3 \\
& + x_{24} I\otimes\sigma_2\otimes\sigma_3 + \ x_{25}\sigma_3\otimes\sigma_2\otimes I \\
& + x_{26}\sigma_3\otimes I\otimes\sigma_2 + x_{27} I\otimes\sigma_3\otimes\sigma_2 \\
& + \ x_{28}\sigma_1\otimes\sigma_1\otimes I + x_{29}\sigma_2\otimes\sigma_2\otimes I \\
& + x_{30}\sigma_3\otimes\sigma_3\otimes I + \ x_{31}\sigma_1\otimes I\otimes\sigma_1 \\
& + x_{32}\sigma_2\otimes I\otimes\sigma_2 + x_{33}\sigma_3\otimes I\otimes\sigma_3 \\
& + \ x_{34} I\otimes\sigma_1\otimes\sigma_1 + x_{35} I\otimes\sigma_2\otimes\sigma_2 \\
& + x_{36} I\otimes\sigma_3\otimes\sigma_3, \qquad (1.8)
\end{aligned}$$

in which $\otimes$ denotes the tensor product, and

$$\begin{aligned}
Q(H) = {} & x_{37}\sigma_1\otimes\sigma_2\otimes\sigma_3 + x_{38}\sigma_1\otimes\sigma_3\otimes\sigma_2 \\
& + \ x_{39}\sigma_2\otimes\sigma_1\otimes\sigma_3 + x_{40}\sigma_2\otimes\sigma_3\otimes\sigma_1 \\
& + \ x_{41}\sigma_3\otimes\sigma_1\otimes\sigma_2 + x_{42}\sigma_3\otimes\sigma_2\otimes\sigma_1 \\
& + \ x_{43}\sigma_1\otimes\sigma_1\otimes\sigma_2 + x_{44}\sigma_1\otimes\sigma_2\otimes\sigma_1 \\
& + \ x_{45}\sigma_2\otimes\sigma_1\otimes\sigma_1 + \ x_{46}\sigma_1\otimes\sigma_1\otimes\sigma_3 \\
& + \ x_{47}\sigma_1\otimes\sigma_3\otimes\sigma_1 + x_{48}\sigma_3\otimes\sigma_1\otimes\sigma_1 \\
& + \ x_{49}\sigma_2\otimes\sigma_2\otimes\sigma_1 + x_{50}\sigma_2\otimes\sigma_1\otimes\sigma_2 \\
& + \ x_{51}\sigma_1\otimes\sigma_2\otimes\sigma_2 + \ x_{52}\sigma_2\otimes\sigma_2\otimes\sigma_3 \\
& + \ x_{53}\sigma_2\otimes\sigma_3\otimes\sigma_2 + x_{54}\sigma_3\otimes\sigma_2\otimes\sigma_2 \\
& + \ x_{55}\sigma_3\otimes\sigma_3\otimes\sigma_1 + x_{56}\sigma_3\otimes\sigma_1\otimes\sigma_3 \\
& + \ x_{57}\sigma_1\otimes\sigma_3\otimes\sigma_3 + \ x_{58}\sigma_3\otimes\sigma_3\otimes\sigma_2 \\
& + \ x_{59}\sigma_3\otimes\sigma_2\otimes\sigma_3 + x_{60}\sigma_2\otimes\sigma_3\otimes\sigma_3 \\
& + \ x_{61}\sigma_1\otimes\sigma_1\otimes\sigma_1 + x_{62}\sigma_2\otimes\sigma_2\otimes\sigma_2 \\
& + \ x_{63}\sigma_3\otimes\sigma_3\otimes\sigma_3. \qquad (1.9)
\end{aligned}$$

Here, all possible tensor products of one and two-qubit Pauli matrix operators on three qubits appear in $P(H)$, and analogously, all possible tensor products of three-qubit operators appear in $Q(H)$. Tensor products including only the identity are excluded because the Hamiltonian is taken to be traceless. Each of the terms in Eqs.

(1.8) and (1.9) is an 8×8 matrix. The various tensor products of Pauli matrices such as those appearing in Eqs. (1.8) and (1.9) are referred to as generalized Pauli matrices. In the case of an n-qubit Hamiltonian, there are $4^n - 1$ possible tensor products (corresponding to the dimension of $SU(2^n)$), and each term is a 2^nx2^n matrix.

The right-invariant [**7**]-[**9**], [**17**], [**18**] Riemannian metric for tangent vectors H and J is given by [**1**]

$$\langle H, J\rangle \equiv \frac{1}{2^n}\mathrm{Tr}\left[HP(J) + qHQ(J)\right]. \tag{1.10}$$

Here q is a large penalty parameter which taxes more than two-body terms. The length l of an evolutionary path on the $SU(2^n)$ manifold is given by the integral over time t from an initial time t_i to a final time t_f, namely,

$$l = \int_{t_i}^{t_f} dt\left(\langle H(t), H(t)\rangle\right)^{1/2}, \tag{1.11}$$

and is a measure of the cost, in terms of quantum circuit complexity, of applying a control Hamiltonian $H(t)$ along the path [**1**].

2. COVARIANT DERIVATIVE

In order to obtain the Levi-Civita connection, one exploits the Lie algebra $su(2^n)$ associated with the group $SU(2^n)$. Because of the right-invariance of the metric, if the connection is calculated at the origin, the same expression applies everywhere on the manifold. Following [**1**], consider the unitary transformation

$$U = e^{-iX} \tag{2.1}$$

in the neighborhood of the identity $I \subset SU(2^n)$ with

$$X = x \cdot \sigma \equiv \sum_{\sigma} x_\sigma \sigma. \tag{2.2}$$

Equation (2.2) expresses symbolically terms like those in Eqs. (1.8) and (1.9) generalized to 2^n dimensions. In Eqs. (2.1) and (2.2), X is defined in terms of U using the standard branch of the logarithm with a cut along the negative real axis. In Eq. (2.2), for the general case of n qubits, x represents the set of real $(4^n - 1)$ coefficients of the generalized Pauli matrices σ which represent all of the n-fold tensor products. Taking the trace of Eq. (2.2), it follows that the factor x^σ multiplying a particular term σ is given by

$$x^\sigma = \frac{1}{2^n}\mathrm{Tr}(X\sigma). \tag{2.3}$$

The right-invariant metric, Eq. (1.10) can be written as

$$\langle H, J\rangle = \frac{1}{2^n}\mathrm{Tr}[HG(J)], \tag{2.4}$$

in which the positive self-adjoint superoperator G is given by

$$G = P + qQ. \tag{2.5}$$

Using Eqs. (1..2) and (2.5), it follows that

$$F \equiv G^{-1} = P + q^{-1}Q. \tag{2.6}$$

A vector Y in the group tangent space can be written as

$$Y = \sum_{\sigma} y^{\sigma} \sigma \tag{2.7}$$

with so-called Pauli coordinates y^{σ}. Here σ, as an index, is used to refer to a particular tensor product appearing in the generalized Pauli matrix σ. This index notation, used throughout, is a convenient abbreviation for the actual numerical indices (e.g. in Eq. (1.9), the number 57 appearing in x_{57}, the coefficient of $\sigma_1 \otimes \sigma_3 \otimes \sigma_3$).

Next consider a curve passing through the origin with tangent vector Y having components $y^{\sigma} = dx^{\sigma}/dt$. It can be shown that the covariant derivative of a right-invariant vector field Z along the curve in the Hamiltonian representation is given by [**1**],[**2**]

$$(\nabla_Y Z) = \frac{i}{2}\{[Y,Z] + F([Y,G(Z)] + [Z,G(Y)])\}. \tag{2.8}$$

Because of the right-invariance of the metric, Eq. (2.8) is true everywhere on the manifold.

3. RIEMANN CURVATURE

The Riemann curvature on the group manifold effects the behavior of geodesics and can be obtained as follows. In the case of a right-invariant vector field Z, one has after substituting

$$Z = \sum_{\tau} z^{\tau} \tau, \quad Y = \sum_{\sigma} y^{\sigma} \sigma \tag{3.1}$$

in Eq. (2.8),

$$\nabla_{\sigma} \tau = \frac{i}{2}\left([\sigma,\tau] + F([\sigma,G(\tau)] + [\tau,G(\sigma)])\right). \tag{3.2}$$

Next denote S_0 as a set containing only tensor products of the identity, and S_{12} as the set of terms in the Hamiltonian containing only one and two body terms, that is

$$S_0 \equiv \{I \otimes I \otimes ...\}, \tag{3.3}$$

and

$$\begin{aligned} S_{12} &= \{I \otimes I \otimes ...\sigma_i \otimes I.., ..\} \\ &\cup \{I \otimes I \otimes ...\sigma_i \otimes I..\sigma_j \otimes I.., ..\}. \end{aligned} \tag{3.4}$$

Evidently then

$$[\sigma, G(\tau)] = \begin{cases} [\sigma,\tau], & \tau \in S_{12} \cup S_0 \\ q[\sigma,\tau], & \tau \notin S_{12} \cup S_0 \end{cases}, \tag{3.5}$$

and therefore

$$F\left([\sigma, G(\tau)]\right) = \begin{cases} F([\sigma,\tau]), & \tau \in S_{12} \cup S_0 \\ qF([\sigma,\tau]), & \tau \notin S_{12} \cup S_0 \end{cases}. \tag{3.6}$$

Using Eq. (2.6) in Eq. (3.6), one obtains

$$F\left([\sigma, G(\tau)]\right) = \begin{cases} \frac{1}{q_{[\sigma,\tau]}}[\sigma,\tau], & \tau \in S_{12} \cup S_0 \\ \frac{q}{q_{[\sigma,\tau]}}[\sigma,\tau], & \tau \notin S_{12} \cup S_0 \end{cases}, \tag{3.7}$$

where

$$q_{[\sigma,\tau]} = 1 \text{ if } [\sigma,\tau] = 0, \quad q_{[\sigma,\tau]} = q_\lambda \text{ if } [\sigma,\tau] \propto \lambda, \text{ and } q_{[\sigma,\tau]} = q_{[\tau,\sigma]}, \tag{3.8}$$

and q_λ is defined by

$$q_\sigma \equiv \begin{cases} 0, & \sigma \in S_0 \\ 1, & \sigma \in S_{12} \\ q, & \sigma \notin S_0 \cup S_{12} \end{cases} . \tag{3.9}$$

Equation (3.7) can also be written as

$$F([\sigma, G(\tau)]) = \frac{q_\tau}{q_{[\sigma,\tau]}}[\sigma,\tau]. \tag{3.10}$$

Next substituting Eq. (3.10) in Eq. (3.2), and using Eq. (3.8), one obtains

$$\nabla_\sigma \tau = i c_{\sigma,\tau}[\sigma,\tau], \tag{3.11}$$

where

$$c_{\sigma,\tau} = \frac{1}{2}\left(1 + \frac{q_\tau - q_\sigma}{q_{[\sigma,\tau]}}\right). \tag{3.12}$$

The Riemann curvature tensor with the inner-product (metric) Eq. (2.4) is given by [**20**]

$$R(W,X,Y,Z) = \left\langle \nabla_W \nabla_X Y - \nabla_X \nabla_W Y - \nabla_{i[W,X]} Y, Z \right\rangle. \tag{3.13}$$

After substituting the vector fields,

$$W = \sum_\sigma w^\rho \rho, \quad X = \sum_\sigma z^\sigma \sigma, \quad Y = \sum_\tau y^\tau \tau, \quad Z = \sum_\mu z^\mu \mu, \tag{3.14}$$

Eq. (3.13) becomes

$$R_{\rho\sigma\tau\mu} = \left\langle \nabla_\rho \nabla_\sigma \tau - \nabla_\sigma \nabla_\rho \tau - \nabla_{i[\rho,\sigma]}\tau, \mu \right\rangle. \tag{3.15}$$

Next, for three right-invariant vector fields X, Y, and Z, one has

$$0 = \nabla_Y \langle X, Z\rangle = \langle X, \nabla_Y Z\rangle + \langle \nabla_Y X, Z\rangle, \tag{3.16}$$

or

$$\langle X, \nabla_Y Z\rangle = -\langle \nabla_Y X, Z\rangle, \tag{3.17}$$

and substituting Eqs. (3.14) in Eq. (3.17), one then has

$$\langle \sigma, \nabla_\tau \mu\rangle = -\langle \nabla_\tau \sigma, \mu\rangle. \tag{3.18}$$

Then replacing the vector σ in Eq. (3.18) by the vector $\nabla_\sigma \tau$, Eq. (3.11) (See Eq. (1.7)), one has

$$\langle \nabla_\rho \nabla_\sigma \tau, \mu\rangle = -\langle \nabla_\sigma \tau, \nabla_\rho \mu\rangle, \tag{3.19}$$

and interchanging indices ρ and σ, then

$$\langle \nabla_\sigma \nabla_\rho \tau, \mu\rangle = -\langle \nabla_\rho \tau, \nabla_\sigma \mu\rangle. \tag{3.20}$$

Then substituting Eqs. (3.19) and (3.20) in Eq. (3.15), and interchanging the first and second terms, one obtains

$$R_{\rho\sigma\tau\mu} = \langle \nabla_\rho \tau, \nabla_\sigma \mu\rangle - \langle \nabla_\sigma \tau, \nabla_\rho \mu\rangle - \left\langle \nabla_{i[\rho,\sigma]}\tau, \mu \right\rangle. \tag{3.21}$$

Also clearly

$$\nabla_{iY} Z = i \nabla_Y Z, \tag{3.22}$$

so Eq. (3.21) can also be written as

$$R_{\rho\sigma\tau\mu} = \langle \nabla_\rho \tau, \nabla_\sigma \mu \rangle - \langle \nabla_\sigma \tau, \nabla_\rho \mu \rangle - i \left\langle \nabla_{[\rho,\sigma]} \tau, \mu \right\rangle . \tag{3.23}$$

Next substituting Eq. (3.11) in Eq. (3.23), one obtains the following useful form for the Riemann curvature tensor [**1**]:

$$\begin{aligned} R_{\rho\sigma\tau\mu} &= c_{\rho,\tau} c_{\sigma,\mu} \langle i[\rho,\tau], i[\sigma,\mu] \rangle \\ &\quad - c_{\sigma,\tau} c_{\rho,\mu} \langle i[\sigma,\tau], i[\rho,\mu] \rangle \\ &\quad - c_{[\rho,\sigma],\tau} \langle i[i[\rho,\sigma],\tau], \mu \rangle . \end{aligned} \tag{3.24}$$

4. GEODESIC EQUATION

The geodesic equation on the $SU(2^n)$ group manifold with the Riemannian metric, Eq. (2.4), is obtained as follows. Consider a curve passing through the origin with tangent vector Y having components $y^\sigma = dx^\sigma/dt$. The covariant derivative along the curve in the Hamiltonian representation is given by [**1**], [**2**].

$$(D_t Z) \equiv (\nabla_Y Z) = \frac{dZ}{dt} + \frac{i}{2} \left([Y, Z] + F \left([Y, G(Z)] + [Z, G(Y)] \right) \right) . \tag{4.1}$$

(Note that the term $\frac{dZ}{dt}$ in Eq. (4.1) does not appear in Eq. (2.8) because there the vector field Z is taken to be right invariant, in which case $\frac{dZ}{dt} = 0$.). Equation (4.1) is true on the entire manifold because of the right-invariance of the metric. Furthermore, a geodesic in the $SU(2^n)$ manifold is a curve $U(t)$ with tangent vector $H(t)$ parallel transported along the curve, namely,

$$D_t H = 0. \tag{4.2}$$

However, according to Eq. (4.1) with $Y = Z = H$, one has

$$D_t H = \frac{dH}{dt} + \frac{i}{2} ([H, H] + F \left([H, G(H)] + [H, G(H)] \right)), \tag{4.3}$$

which when substituting Eq. (4.2) becomes [**1**]

$$\frac{dH}{dt} = -iF \left([H, G(H)] \right) . \tag{4.4}$$

One can rewrite Eq. (4.4) using the dual L of H [**1**], [**2**] and Eq. (2.6),

$$L \equiv G(H) = F^{-1}(H), \tag{4.5}$$

and then noting that

$$\frac{dL}{dt} = \frac{d}{dt} \left(F^{-1}(H) \right) = F^{-1} \left(\frac{dH}{dt} \right) . \tag{4.6}$$

Thus substituting Eq. (4.4) in Eq. (4.6), one obtains

$$\frac{dL}{dt} = -iF^{-1} \left(F([H, G(H)]) \right), \tag{4.7}$$

or

$$\frac{dL}{dt} = -i[H, G(H)], \tag{4.8}$$

and again using Eq. (4.5), Eq. (4.8) becomes

$$\frac{dL}{dt} = -i[H, L] = i[L, H]. \tag{4.9}$$

Furthermore, again using Eq. (4.5) in Eq. (4.9), one obtains the sought geodesic equation [**1**]:

$$\frac{dL}{dt} = i[L, F(L)]. \tag{4.10}$$

This equation is a Lax equation, a well-known nonlinear differential matrix equation, and L and $iF(L)$ are Lax pairs [**21**]-[**23**]. Some solutions to the geodesic equation, Eq. (4.10), are given in [**1**].

5. JACOBI FIELDS

Consider a one-parameter family of geodesics on a generic Riemannian manifold,

$$x^j = x^j(s,t), \tag{5.1}$$

in which the parameter s distinguishes a particular geodesic in the family, and t is the usual curve parameter which can be taken to be time. (In this section, Latin indices are used in the description of the Riemannian manifold. Also, the x^j in Eq. (5.1) are not to be confused with the x_σ of Sections 1 and 2.) The Riemannian geodesic equation in a coordinate representation is given by [**9**]

$$\frac{\partial^2 x^j}{\partial t^2} + \Gamma^j_{kl}(s)\frac{\partial x^k}{\partial t}\frac{\partial x^l}{\partial t} = 0, \tag{5.2}$$

in which the Levi-Civita connection is given by,

$$\Gamma^j_{kl}(s) = \frac{1}{2}g^{jm}(s)(g_{km,l}(s) + g_{lm,k}(s) - g_{kl,m}(s)), \tag{5.3}$$

for metric $g_{ij}(x(s,t)) \equiv g_{ij}(s)$. (Partial derivatives are used in Eq. (5.2) to distinguish the s from the t dependence.) The geodesic equation, Eq. (4.10), on the $SU(2^n)$ group manifold can be shown to also follow from Eq. (5.2) [**1**], [**2**].

Let $x^j(0,t)$ be the base geodesic, and define the lifted Jacobi field along the base geodesic by [**1**]

$$J^j(t) = \frac{\partial}{\partial s}x^j(s,t)_{|s=0}, \tag{5.4}$$

describing how the base geodesic changes as the parameter s is varied. Using a Taylor series expansion, one has for small Δs in the neighborhood of the base geodesic,

$$x^j(\Delta s, t) = x^j(0,t) + \Delta s J^j(t) + O(\Delta s^2). \tag{5.5}$$

Here $x^j(\Delta s, t)$ satisfies the geodesic equation with the metric $g_{ij}(\Delta s)$. Operating on the geodesic equation, Eq. (5.2) with $\partial_s \equiv \frac{\partial}{\partial s}$ and substituting Eqs. (5.4) and (5.5), one obtains for $\Delta s \to 0$,

$$\begin{aligned} 0 = {} & \frac{\partial^2}{\partial t^2}\operatorname*{Lim}_{\Delta s\to 0}\frac{\Delta s J^j(t)}{\Delta s} + \Gamma^j_{kl,m}(s)_{|s=0}\operatorname*{Lim}_{\Delta s\to 0}\frac{\Delta s J^m(t)}{\Delta s}\frac{\partial x^k}{\partial t}\frac{\partial x^l}{\partial t} + \partial_s\Gamma^j_{kl}(s)_{|s=0}\frac{\partial x^k}{\partial t}\frac{\partial x^l}{\partial t} \\ & + \Gamma^j_{kl}(0)\left\{\frac{\partial}{\partial t}\left(\operatorname*{Lim}_{\Delta s\to 0}\frac{\Delta s J^k(t)}{\Delta s}\right)\frac{\partial x^l}{\partial t} + \frac{\partial x^k}{\partial t}\frac{\partial}{\partial t}\operatorname*{Lim}_{\Delta s\to 0}\frac{\Delta s J^l(t)}{\Delta s}\right\}, \end{aligned} \tag{5.6}$$

in which $g_{ij}(0) \equiv g_{ij}$ is the base metric and $\Gamma^j_{kl}(0) \equiv \Gamma^j_{kl}$ is the base connection. Equation (5.6) then becomes

$$\begin{aligned} 0 = & \frac{\partial^2 J^j(t)}{\partial t^2} + \Gamma^j_{kl,m}(s)_{|s=0} J^m(t) \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t} \\ & + \partial_s \Gamma^j_{kl}(s)_{|s=0} \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t} + \Gamma^j_{kl} \left(\frac{\partial J^k}{\partial t} \frac{\partial x^l}{\partial t} + \frac{\partial x^k}{\partial t} \frac{\partial J^l}{\partial t} \right). \end{aligned} \tag{5.7}$$

Taking account of dummy indices summed over, it is clearly true that

$$-\Gamma^j_{lq} \Gamma^q_{ik} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k + \Gamma^j_{kp} \Gamma^p_{mn} \frac{\partial x^k}{\partial t} \frac{\partial x^m}{\partial t} J^n = 0. \tag{5.8}$$

One also has

$$-\Gamma^j_{ik,l} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k + \Gamma^j_{kp,m} \frac{\partial x^m}{\partial t} \frac{\partial x^k}{\partial t} J^p = 0. \tag{5.9}$$

Also, using the geodesic equation, Eq. (5.2), one has

$$\Gamma^j_{kp} \frac{\partial^2 x^k}{\partial t^2} J^p = -\Gamma^j_{kp} \Gamma^k_{iq} \frac{\partial x^i}{\partial t} \frac{\partial x^q}{\partial t} J^p, \tag{5.10}$$

or renaming dummy indices on the right hand side, it follows that

$$\Gamma^j_{kp} \frac{\partial^2 x^k}{\partial t^2} J^p + \Gamma^j_{qk} \Gamma^q_{il} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k = 0. \tag{5.11}$$

Next adding Eqs. (5.7)-(5.9) and (5.11), one obtains

$$\begin{aligned} 0 = & \frac{\partial^2 J^j(t)}{\partial t^2} + \Gamma^j_{kl,m} J^m(t) \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t} \\ & + \partial_s \Gamma^j_{kl}(s)_{|s=0} \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t} + \Gamma^j_{kl} \left(\frac{\partial J^k}{\partial t} \frac{\partial x^l}{\partial t} + \frac{\partial x^k}{\partial t} \frac{\partial J^l}{\partial t} \right) \\ & - \Gamma^j_{lq} \Gamma^q_{lk} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k + \Gamma^j_{kp} \Gamma^p_{mn} \frac{\partial x^k}{\partial t} \frac{\partial x^m}{\partial t} J^n \\ & - \Gamma^j_{ik,l} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k + \Gamma^j_{kp,m} \frac{\partial x^m}{\partial t} \frac{\partial x^k}{\partial t} J^p + \Gamma^j_{kp} \frac{\partial^2 x^k}{\partial t^2} J^p + \Gamma^j_{qk} \Gamma^q_{il} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k, \end{aligned} \tag{5.12}$$

or equivalently,

$$\begin{aligned} \frac{\partial^2 J^j(t)}{\partial t^2} = & - \Gamma^j_{kl,m} \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t} J^m + \Gamma^j_{lq} \Gamma^q_{ik} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k \\ & - \Gamma^j_{kp} \Gamma^p_{mn} \frac{\partial x^k}{\partial t} \frac{\partial x^m}{\partial t} J^n - \Gamma^j_{qk} \Gamma^q_{il} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k + \Gamma^j_{ik,l} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k \\ & - \Gamma^j_{kp} \frac{\partial^2 x^k}{\partial t^2} J^p - \Gamma^j_{kl} \left(\frac{\partial J^k}{\partial t} \frac{\partial x^l}{\partial t} + \frac{\partial x^k}{\partial t} \frac{\partial J^l}{\partial t} \right) \\ & - \partial_s \Gamma^j_{kl}(s)_{|s=0} \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t} - \Gamma^j_{kp,m} \frac{\partial x^m}{\partial t} \frac{\partial x^k}{\partial t} J^p. \end{aligned} \tag{5.13}$$

Rearranging terms in Eq. (5.13), then

$$\begin{aligned}\frac{\partial^2 J^j(t)}{\partial t^2} &= \Gamma^j_{ik,l}\frac{\partial x^i}{\partial t}\frac{\partial x^l}{\partial t}J^k - \Gamma^j_{kl,m}\frac{\partial x^k}{\partial t}\frac{\partial x^l}{\partial t}J^m + \Gamma^j_{lq}\Gamma^q_{ik}\frac{\partial x^i}{\partial t}\frac{\partial x^l}{\partial t}J^k \\ &\quad - \Gamma^j_{kp}\Gamma^p_{mn}\frac{\partial x^k}{\partial t}\frac{\partial x^m}{\partial t}J^n - \Gamma^j_{kp,m}\frac{\partial x^m}{\partial t}\frac{\partial x^k}{\partial t}J^p - \Gamma^j_{kp}\frac{\partial^2 x^k}{\partial t^2}J^p \\ &\quad - \Gamma^j_{kl}\frac{\partial x^k}{\partial t}\frac{\partial J^l}{\partial t} - \Gamma^j_{kl}\frac{\partial x^l}{\partial t}\frac{\partial J^k}{\partial t} \\ &\quad - \Gamma^j_{qk}\Gamma^q_{il}\frac{\partial x^i}{\partial t}\frac{\partial x^l}{\partial t}J^k - \partial_s\Gamma^j_{kl}(s)_{|s=0}\frac{\partial x^k}{\partial t}\frac{\partial x^l}{\partial t}. \end{aligned} \tag{5.14}$$

Recalling that the Levi-Civita connection is symmetric, one has

$$\Gamma^j_{qp} = \Gamma^j_{pq}, \tag{5.15}$$

and renaming dummy indices, Eq. (5.14) becomes

$$\begin{aligned}\frac{\partial^2 J^j}{\partial t^2} &= \left(\Gamma^j_{ik,l} - \Gamma^j_{il,k} + \Gamma^j_{lq}\Gamma^q_{ik} - \Gamma^j_{kp}\Gamma^p_{li}\right)\frac{\partial x^i}{\partial t}\frac{\partial x^l}{\partial t}J^k \\ &\quad - \Gamma^j_{kp,m}\frac{\partial x^m}{\partial t}\frac{\partial x^k}{\partial t}J^p - \Gamma^j_{kp}\frac{\partial^2 x^k}{\partial t^2}J^p - \Gamma^j_{kl}\frac{\partial x^k}{\partial t}\frac{\partial J^l}{\partial t} \\ &\quad - \Gamma^j_{pk}\frac{\partial x^k}{\partial t}\left(\frac{\partial J^p}{\partial t} + \Gamma^p_{mn}\frac{\partial x^m}{\partial t}J^n\right) - \partial_s\Gamma^j_{kl}(s)_{|s=0}\frac{\partial x^k}{\partial t}\frac{\partial x^l}{\partial t}. \end{aligned} \tag{5.16}$$

Using the well-known expression for the covariant derivative [**13**], [**20**], it follows that

$$\begin{aligned}\frac{D^2 J^j}{Dt^2} &= \frac{\partial}{\partial t}\left(\frac{DJ^j}{Dt}\right) + \Gamma^j_{kp}\frac{\partial x^k}{\partial t}\frac{DJ^p}{Dt} \\ &= \frac{\partial}{\partial t}\left(\frac{\partial J^j}{\partial t} + \Gamma^j_{kp}\frac{\partial x^k}{\partial t}J^p\right) + \Gamma^j_{kp}\frac{\partial x^k}{\partial t}\frac{DJ^p}{Dt}, \end{aligned} \tag{5.17}$$

or

$$\begin{aligned}\frac{D^2 J^j}{Dt^2} &= \frac{\partial^2 J^j}{\partial t^2} + \Gamma^j_{kp,m}\frac{\partial x^m}{\partial t}\frac{\partial x^k}{\partial t}J^p + \Gamma^j_{kp}\frac{\partial^2 x^k}{\partial t^2}J^p + \Gamma^j_{kp}\frac{\partial x^k}{\partial t}\frac{\partial J^p}{\partial t} \\ &\quad + \Gamma^j_{kp}\frac{\partial x^k}{\partial t}\left(\frac{\partial J^p}{\partial t} + \Gamma^p_{mn}\frac{\partial x^m}{\partial t}J^n\right). \end{aligned} \tag{5.18}$$

Next the well-known Riemann curvature tensor is given by [**20**]

$$R^j_{ikl} = \Gamma^j_{il,k} - \Gamma^j_{ik,l} + \Gamma^j_{kp}\Gamma^p_{li} - \Gamma^j_{lq}\Gamma^q_{ik}. \tag{5.19}$$

Substituting Eqs. (5.16) and (5.19) in Eq. (5.18), one obtains the so-called lifted Jacobi equation [**1**],

$$\frac{D^2 J^j}{Dt^2} + R^j_{ikl}\frac{\partial x^i}{\partial t}\frac{\partial x^l}{\partial t}J^k + \partial_s\Gamma^j_{kl}(s)_{|s=0}\frac{\partial x^k}{\partial t}\frac{\partial x^l}{\partial t} = 0. \tag{5.20}$$

This equation is useful for investigations of the global behavior of geodesics and their extrapolation to values of the parameter s characterizing neighboring geodesics on the Riemannian manifold [**1**].

If g_{ij} is independent of s, one has

$$\partial_s\Gamma^j_{kl}(s)_{|s=0} = 0, \tag{5.21}$$

the last term of Eq. (5.20) is then vanishing, and one obtains the standard Jacobi equation for the Jacobi vector J^j [**9**],

$$\frac{D^2 J^j}{Dt^2} + R^j_{ikl}\frac{\partial x^i}{\partial t}\frac{\partial x^l}{\partial t}J^k = 0. \tag{5.22}$$

Equation (5.22) is also known as the equation of geodesic deviation [**24**],[**20**], measuring the local convergence or divergence of neighboring geodesics, and it is useful in the determination of possible geodesic conjugate points [**9**], [**1**].(Conjugate points are points on a geodesic at which the Jacobi field is vanishing without vanishing in between those points.) It is well-known that past the first conjugate point, a geodesic ceases to be minimizing [**6**], [**9**].

Next consider the factor in the last term of the lifted Jacobi equation, Eq. (5.20),

$$L^j_{kl} \equiv \partial_s \Gamma^j_{kl}(s)_{|s=0}. \tag{5.23}$$

Substituting Eq. (5.3) in Eq. (5.23), one has

$$L^j_{kl} \equiv \left\{\partial_s \left[\frac{1}{2}g^{jm}(s)(g_{km,l}(s) + g_{lm,k}(s) - g_{kl,m}(s)\right]\right\}_{|s=0}, \tag{5.24}$$

or equivalently,

$$L^j_{kl} \equiv \frac{\partial g^{jm}(s)}{\partial s}_{|s=0}\Gamma_{mkl} + \frac{1}{2}g^{jm}(g'_{km,l} + g'_{lm,k} - g'_{kl,m}), \tag{5.25}$$

in which one defines

$$g'_{km} \equiv \partial_s g_{km}(s)_{|s=0}. \tag{5.26}$$

Using the well-known expression for the covariant derivative of a second rank tensor [**20**], one has

$$g'_{km;l} = g'_{km,l} - g'_{ki}\Gamma^i_{ml} - g'_{mi}\Gamma^i_{kl}. \tag{5.27}$$

Then substituting Eq. (5.27) in Eq. (5.25), one obtains

$$\begin{aligned} L^j_{kl} \equiv \frac{\partial g^{jm}(s)}{\partial s}_{|s=0}\Gamma_{mkl} + \frac{1}{2}g^{jm}(&g'_{km;l} + g'_{ki}\Gamma^i_{ml} + g'_{mi}\Gamma^i_{kl} \\ &+ g'_{lm;k} + g'_{li}\Gamma^i_{mk} + g'_{mi}\Gamma^i_{kl} \\ &- g'_{kl;m} - g'_{ki}\Gamma^i_{lm} - g'_{li}\Gamma^i_{km}), \end{aligned} \tag{5.28}$$

and using Eq. (5.15), then

$$\begin{aligned} L^j_{kl} \equiv &\frac{1}{2}g^{jm}(g'_{km;l} + g'_{lm;k} - g'_{kl;m}) \\ &+ \frac{\partial g^{jm}(s)}{\partial s}_{|s=0}\Gamma_{mkl} + g^{jm}g'_{mi}\Gamma^i_{kl}. \end{aligned} \tag{5.29}$$

Next noting that

$$(g^{jm}g_{mi})' = (\delta^j_i)' = 0, \tag{5.30}$$

then

$$g^{jm}(0)\left(\frac{\partial}{\partial s}g_{mi}(s)\right)_{|s=0} = -\left(\frac{\partial g^{jm}(s)}{\partial s}\right)_{|s=0} g_{mi}(0). \tag{5.31}$$

Multiplying both sides of Eq. (5.31) by Γ^i_{kl}, and using Eq. (5.26), one obtains

$$g^{jm} g'_{mi} \Gamma^i_{kl} = - \left(\frac{\partial g^{jm}(s)}{\partial s} \right)_{|s=0} \Gamma_{mkl}, \tag{5.32}$$

so that Eq. (5.29) reduces to

$$L^j_{kl} \equiv \frac{1}{2} g^{jm} (g'_{km;l} + g'_{lm;k} - g'_{kl;m}). \tag{5.33}$$

Finally then combining Eqs. (5.20), (5.23) and (5.33), one obtains

$$\frac{D^2 J^j}{Dt^2} + R^j_{ikl} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k + \frac{1}{2} g^{jm} (g'_{km;l} + g'_{lm;k} - g'_{kl;m}) \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t} = 0. \tag{5.34}$$

Next define the vector field,

$$C^j \equiv \frac{1}{2} g^{jm} (g'_{km;l} + g'_{lm;k} - g'_{kl;m}) \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t}, \tag{5.35}$$

which is independent of the Jacobi field J^j. Equivalently, by symmetry, Eq. (5.35) can also be written as

$$C^j \equiv \frac{1}{2} g^{jm} (2 g'_{km;l} - g'_{kl;m}) \frac{\partial x^k}{\partial t} \frac{\partial x^l}{\partial t}. \tag{5.36}$$

Substituting Eq. (5.35) in Eq. (5.34), one obtains the second-order differential equation,

$$\frac{D^2 J^j}{Dt^2} + R^j_{ikl} \frac{\partial x^i}{\partial t} \frac{\partial x^l}{\partial t} J^k + C^j = 0, \tag{5.37}$$

the so-called 'lifted Jacobi equation' [**1**]. Nielsen and Dowling used the lifted Jacobi equation, Eq. (5.37), adapted to the $SU(2^n)$ group manifold, to deform geodesics by varying the penalty parameter q (See the following Section.). This enabled them to define a so-called 'geodesic derivative' and to numerically deform a geodesic as the penalty parameter q is varied without changing the fixed values $U = 1$ and $U = U_f$ of the initial and final unitary transformation corresponding to a quantum computation [**1**].

The generic lifted Jacobi equation, Eq. (5.37) can be solved. One first rewrites Eq. (5.18) as

$$\begin{aligned} \frac{D^2 J^j}{Dt^2} &= \frac{\partial^2 J^j}{\partial t^2} + 2\Gamma^j_{kp} \frac{\partial x^k}{\partial t} \frac{\partial J^p}{\partial t} + \Gamma^j_{kp,m} \frac{\partial x^m}{\partial t} \frac{\partial x^k}{\partial t} J^p + \Gamma^j_{kp} \frac{\partial^2 x^k}{\partial t^2} J^p \\ &\quad + \Gamma^j_{kp} \frac{\partial x^k}{\partial t} \Gamma^p_{mn} \frac{\partial x^m}{\partial t} J^n, \end{aligned} \tag{5.38}$$

and renaming dummy indices in the last term, then

$$\begin{aligned} \frac{D^2 J^j}{Dt^2} &= \frac{\partial^2 J^j}{\partial t^2} + \left(2\Gamma^j_{kp} \frac{\partial x^k}{\partial t} \right) \frac{\partial J^p}{\partial t} \\ &\quad + \left(\Gamma^j_{kp,m} \frac{\partial x^m}{\partial t} \frac{\partial x^k}{\partial t} + \Gamma^j_{kp} \frac{\partial^2 x^k}{\partial t^2} + \Gamma^j_{kq} \frac{\partial x^k}{\partial t} \Gamma^q_{mp} \frac{\partial x^m}{\partial t} \right) J^p, \end{aligned} \tag{5.39}$$

or equivalently

$$\frac{D^2 J^j}{Dt^2} = \frac{\partial^2 J^j}{\partial t^2} + A^j_p \frac{\partial J^p}{\partial t} + \left(\sum_{n=1}^{3} {}^{(n)}B^j_p \right) J^p \tag{5.40}$$

where

$$A_p^j \equiv \left(2\Gamma_{kp}^j \frac{\partial x^k}{\partial t}\right), \tag{5.41}$$

$${}^{(1)}B_p^j \equiv \Gamma_{kp,m}^j \frac{\partial x^m}{\partial t}\frac{\partial x^k}{\partial t}, \tag{5.42}$$

$${}^{(2)}B_p^j \equiv \Gamma_{kp}^j \frac{\partial^2 x^k}{\partial t^2}, \tag{5.43}$$

and

$${}^{(3)}B_p^j \equiv \Gamma_{kq}^j \frac{\partial x^k}{\partial t}\Gamma_{mp}^q \frac{\partial x^m}{\partial t}. \tag{5.44}$$

Next Eq. (5.37) can written as

$$\frac{D^2 J^j}{Dt^2} + {}^{(4)}B_p^j J^p + C^j = 0, \tag{5.45}$$

where

$${}^{(4)}B_p^j \equiv R_{ipl}^j \frac{\partial x^i}{\partial t}\frac{\partial x^l}{\partial t}. \tag{5.46}$$

Next substituting Eq. (5.45) in Eq. (5.40), one obtains

$$\frac{\partial^2 J^j}{\partial t^2} + A_p^j \frac{\partial J^p}{\partial t} + B_p^j J^p + C^j = 0, \tag{5.47}$$

where

$$B_p^j = \sum_{n=1}^{4} {}^{(n)}B_p^j. \tag{5.48}$$

Next define the column vectors

$$J \equiv \left[J^j\right], \tag{5.49}$$

$$C \equiv \left[C^j\right], \tag{5.50}$$

and the matrices

$$A \equiv \left[A_p^j\right], \tag{5.51}$$

$$B \equiv \left[B_p^j\right] = \left[\sum_{n=1}^{4} {}^{(n)}B_p^j.\right]. \tag{5.52}$$

Equation (5.47) then becomes

$$\frac{\partial^2 J}{\partial t^2} + A\frac{\partial J}{\partial t} + BJ + C = 0. \tag{5.53}$$

Furthermore defining the column vector

$$K \equiv \begin{bmatrix} J_1 \\ J_2 \end{bmatrix} \equiv \begin{bmatrix} J \\ \frac{\partial J}{\partial t} \end{bmatrix}, \tag{5.54}$$

then Eq. (5.53) is equivalent to

$$\frac{\partial K}{\partial t} \equiv \begin{bmatrix} 0 & I \\ -B & -A \end{bmatrix} K - \begin{bmatrix} 0 \\ C \end{bmatrix}. \tag{5.55}$$

The homogeneous part of Eq. (5.55) with $C = 0$ is equivalent to the Jacobi equation, Eq. (5.22), and is given by

$$\frac{\partial K_0}{\partial t} \equiv M K_0, \tag{5.56}$$

in which the matrix M is given by

$$M \equiv \begin{bmatrix} 0 & I \\ -B(t) & -A(t) \end{bmatrix}, \tag{5.57}$$

and the time dependence of A and B is indicated explicitly. The solution to the Jacobi equation, Eq. (5.56), is given in terms of the time-ordered exponential [**25**],[**26**] namely,

$$K_0(t) = \left(I + \sum_{n=1}^{\infty} \frac{1}{n!} \int_0^t dt_1 .. \int_0^t dt_n \mathrm{T}(M(t_1)...M(t_n)) \right) K_0(0), \tag{5.58}$$

where T denotes the time ordering operator (not to be confused with the transpose of a matrix, appearing below). Thus, Eq. (5.58) gives the Jacobi field and can be expressed formally as

$$K_0(t) = \mathrm{T} \exp \left(\int_0^t dt' M(t') \right) K_0(0), \tag{5.59}$$

or defining the operator

$$E_t \equiv \mathrm{T} \exp \left(\int_0^t dt' M(t') \right) = I + \sum_{n=1}^{\infty} \frac{1}{n!} \int_0^t dt_1 .. \int_0^t dt_n \mathrm{T}(M(t_1)...M(t_n)), \tag{5.60}$$

Equation (5.59) can also be written as

$$K_0(t) = E_t K_0(0), \tag{5.61}$$

It follows from Eq. (5.60) that

$$\begin{aligned} \frac{\partial E_t}{\partial t} &= M(t) + \sum_{n=2}^{\infty} \frac{1}{n!} n \int_0^t dt_1 .. \int_0^t dt_{n-1} \mathrm{T}(M(t_1)...M(t_{n-1})M(t)) \\ &= M(t) + M(t) \sum_{n=2}^{\infty} \frac{1}{(n-1)!} \int_0^t dt_1 .. \int_0^t dt_{n-1} \mathrm{T}(M(t_1)...M(t_{n-1})) \\ &= M(t) \left(I + \sum_{n=1}^{\infty} \frac{1}{n!} \int_0^t dt_1 .. \int_0^t dt_n \mathrm{T}(M(t_1)...M(t_n)) \right), \end{aligned} \tag{5.62}$$

or equivalently then substituting Eq. (5.60), one obtains

$$\frac{\partial E_t}{\partial t} = M(t) E_t. \tag{5.63}$$

The solution to the inhomogeneous equation, Eq. (5.55) is given by

$$K(t) = E_t K(0) - E_t \int_0^t dr E_r^{-1} \begin{bmatrix} 0 \\ C(r) \end{bmatrix}, \tag{5.64}$$

This is the lifted Jacobi field. To see that Eq, (5.64) solves the inhomogeneous equation, Eq. (5.55), one notes that using Eqs. (5.64) and (5.63) one has

$$\frac{\partial K(t)}{\partial t} = \frac{\partial E_t}{\partial t}K(0) - \frac{\partial E_t}{\partial t}\int_0^t dr E_r^{-1}\begin{bmatrix}0\\C(r)\end{bmatrix} - E_t E_t^{-1}\begin{bmatrix}0\\C(t)\end{bmatrix}$$

$$= M(t)E_t K(0) - M(t)E_t\int_0^t dr E_r^{-1}\begin{bmatrix}0\\C(r)\end{bmatrix} - \begin{bmatrix}0\\C(t)\end{bmatrix}. \tag{5.65}$$

Next substituting Eqs. (5.61), (5.64) and (5.57) in Eq. (5.65), then

$$\frac{\partial K(t)}{\partial t} = M(t)E_t K(0) + M(t)K(t) - M(t)E_t K(0) - \begin{bmatrix}0\\C(t)\end{bmatrix}$$

$$= \begin{bmatrix} 0 & I \\ -B(t) & -A(t)\end{bmatrix} K(t) - \begin{bmatrix}0\\C(t)\end{bmatrix}, \tag{5.66}$$

and thus Eq. (5.55) is in fact satisfied by Eq. (5.64).

6. LIFTED JACOBI EQUATION FOR VARIED PENALTY PARAMETER

Consider a base geodesic with coordinates $\gamma^\sigma(q,t)$ on the $SU(2^n)$ group manifold with penalty parameter q, and a neighboring geodesic with coordinates $\gamma^\sigma(q+\Delta,t)$ with penalty parameter $q+\Delta$. To first order in Δ, one has

$$\gamma^\sigma(q+\Delta,t) = \gamma^\sigma(q,t) + \Delta J^\sigma(t), \tag{6.1}$$

in which the Jacobi field coordinates $J^\sigma(t)$ are defined by

$$J^\sigma(t) = \frac{\partial\gamma^\sigma(q,t)}{\partial q}. \tag{6.2}$$

The Hamiltonian for a geodesic $\gamma(t)$ with penalty parameter q is given by

$$H_q = \frac{d\gamma}{dt}. \tag{6.3}$$

Then one has

$$\frac{dH_q}{dq} = \frac{d}{dq}\frac{d\gamma}{dt}, \tag{6.4}$$

or equivalently,

$$\frac{dH_q}{dq} = \frac{d}{dt}\frac{d\gamma}{dq}, \tag{6.5}$$

and substituting Eq. (6.2) in Eq. (6.5), then

$$\frac{dH_q}{dq} = \frac{dJ}{dt} \tag{6.6}$$

in which the Jacobi field J is

$$J = J^\sigma\sigma. \tag{6.7}$$

The geodesic equation for the base geodesic with penalty parameter q is given by Eq. (4.9), namely,

$$\frac{dL}{dt} = i[L,H], \tag{6.8}$$

where the dual L is given by

$$L = G(H). \tag{6.9}$$

The geodesic equation for the nearby geodesic with penalty parameter $q + \Delta$ is

$$\frac{d\overline{L}}{dt} = i[\overline{L}, \overline{H}], \tag{6.10}$$

where

$$\overline{L} = \overline{G}(\overline{H}), \tag{6.11}$$

and in accord with Eq. (2.5),

$$\overline{G} = P + (q + \Delta)Q = G + \Delta\frac{dG}{dq} \equiv G + \Delta G', \tag{6.12}$$

in which

$$G' \equiv \frac{dG}{dq} = Q. \tag{6.13}$$

Next letting $U(t)$ and $\overline{U}(t)$ denote the geodesics for penalty parameter q and $q + \Delta$, respectively, then for small Δ one expects

$$\overline{U} = Ue^{-i\Delta J}, \tag{6.14}$$

and it follows that to first order in Δ,

$$\begin{aligned}\frac{d\overline{U}}{dt} &= \frac{dU}{dt}e^{-i\Delta J} + U\frac{d}{dt}\left(1 - i\Delta J + 0(\Delta^2)\right)\\ &= \frac{dU}{dt}e^{-i\Delta J} + U(-i\Delta\frac{dJ}{dt} + 0(\Delta^2))\\ &= \frac{dU}{dt}e^{-i\Delta J} - iU\Delta\frac{dJ}{dt}.\end{aligned} \tag{6.15}$$

But according to the Schrődinger equation, one has

$$\frac{d\overline{U}}{dt} = -i\overline{HU} \tag{6.16}$$

and

$$\frac{dU}{dt} = -iHU, \tag{6.17}$$

so substituting Eqs. (6.16) and (6.17) in Eq. (6.15), one obtains

$$-i\overline{HU} = -iHUe^{-i\Delta J} - iU\Delta\frac{dJ}{dt}, \tag{6.18}$$

or substituting Eq. (6.14), then Eq. (6.18) for small Δ becomes

$$-i\overline{H}Ue^{-i\Delta J} = -iHUe^{-i\Delta J} - iU\Delta\frac{dJ}{dt}, \tag{6.19}$$

or equivalently, then to order Δ,

$$-i\overline{H}U = -iHU - iU\Delta\frac{dJ}{dt}e^{i\Delta J} = -iHU - iU\Delta\frac{dJ}{dt}. \tag{6.20}$$

Next multiplying Eq. (6.20) on the right by $U^\dagger$ and noting that unitarity requires

$$UU^\dagger = 1, \tag{6.21}$$

then Eq. (6.20) becomes

$$\overline{H} = H + \Delta U \frac{dJ}{dt} U^{\dagger} \tag{6.22}$$

to first order in Δ. Next substituting Eq. (6.11) in Eq. (6.10), one obtains

$$\frac{d}{dt}(\overline{G(H)}) = i[\overline{G(H)}, \overline{H}]. \tag{6.23}$$

Then substituting Eqs. (6.12) and (6.22) in the left side of Eq. (6.23), the left side becomes

$$\frac{d}{dt}(\overline{G(H)}) = \frac{d}{dt}((G + \Delta G')(H + \Delta K)), \tag{6.24}$$

where

$$K \equiv U \frac{dJ}{dt} U^{\dagger}. \tag{6.25}$$

Equivalently, Eq. (6.24) to first order in Δ is

$$\frac{d}{dt}(\overline{G(H)}) = \frac{d}{dt} G(H) + \Delta \frac{d}{dt}(G'(H) + G(K)). \tag{6.26}$$

Next, using Eqs. (6.12), (6.22), and (6.25), the right side of Eq. (6.23) becomes

$$i[\overline{G(H)}, \overline{H})] = i[(G + \Delta G')(H + \Delta K), H + \Delta K], \tag{6.27}$$

or equivalently to first order in Δ,

$$i[\overline{G(H)}, \overline{H})] = i[G(H), H] + \Delta(i[G(H), K] + i[G'(H), H] + i[G(K), H]). \tag{6.28}$$

In terms of the dual, Eq. (6.9), Eq. (6.28) becomes

$$i[\overline{G(H)}, \overline{H})] = i[L, H] + \Delta(i[L, K] + i[G'(H), H] + i[G(K), H]). \tag{6.29}$$

Next substituting Eqs. (6.26), (6.9) and (6.29) in Eq. (6.23), one obtains

$$\frac{d}{dt} L + \Delta(G'(\frac{d}{dt} H) + G(\frac{d}{dt} K)) = i[L, H] + \Delta(i[L, K] + i[G'(H), H] + i[G(K), H]), \tag{6.30}$$

and further substituting Eq. (6.8) in Eq. (6.30), one concludes that

$$G'(\frac{d}{dt} H) + G(\frac{d}{dt} K)) = i[L, K] + i[G'(H), H] + i[G(K), H]. \tag{6.31}$$

Furthermore, multiplying Eq. (6.31) on the left by G^{-1}, one obtains

$$G^{-1} G'(\frac{d}{dt} H) + \frac{d}{dt} K = G^{-1}(i[L, K] + i[G'(H), H] + i[G(K), H]). \tag{6.32}$$

But according to Eqs. (6.8), (6.9), and (2.6),

$$\frac{d}{dt} H = i G^{-1}[L, H] = i F([L, H]), \tag{6.33}$$

so that, using Eq. (2.6), one has

$$G^{-1} G'(\frac{d}{dt} H) = F G'(\frac{d}{dt} H) = i F G' F([L, H]). \tag{6.34}$$

Then substituting Eqs. (6.34) and (2.6) in Eq. (6.32), one obtains

$$0 = i F G' F([L, H]) + \frac{d}{dt} K + \ F(i[K, L] + i[H, G'(H)] + i[H, G(K)]), \tag{6.35}$$

or

$$0 = \frac{d}{dt}K + \ F(i[K,L] + i[H,G(K)] + G'F(i[L,H]) + i[H,G'(H)]). \tag{6.36}$$

Equation (6.36) is the lifted Jacobi equation for penalty parameter varied from q to $q + \Delta$ [**1**]. It is an inhomogeneous first order differential equation in K.

If $G' = 0$, Eq. (6.36) reduces effectively to the conventional Jacobi equation, assuming the form,

$$0 = \frac{d}{dt}K + \ F(i[K,L] + i[H,G(K)]). \tag{6.37}$$

Equation (6.37) can be rewritten as follows using Eqs. (1.2), (2.5), and (2.6):

$$\frac{d}{dt}K = -iF([P(K) + Q(K), P(H) + qQ(H)] + [P(H) + Q(H), P(K) + qQ(K)]). \tag{6.38}$$

Expanding the commutators, then

$$\begin{aligned}\frac{d}{dt}K = -iF([P(K),P(H)] + q[P(K),Q(H)] \\ + [Q(K),P(H)] + q[Q(K),Q(H)] \\ + [P(H),P(K)] + q[P(H),Q(K)] \\ + [Q(H),P(K)] + q[Q(H),Q(K)]).\end{aligned} \tag{6.39}$$

The first and fifth terms cancel, and also the forth and eighth terms cancel, so one obtains

$$\frac{d}{dt}K = -i(q-1)F([P(K),Q(H)] - [Q(K),P(H)]), \tag{6.40}$$

or equivalently,

$$\frac{d}{dt}K = -i(q-1)F([P(K),Q(H)] + [P(H),Q(K)]), \tag{6.41}$$

or

$$\frac{d}{dt}K = i(q-1)F([Q(H),P(K)] - [P(H),Q(K)]). \tag{6.42}$$

Solving Eq. (6.42) for K yields the conventional Jacobi field.

The inhomogeneous term in Eq. (6.36) is given by

$$C = F(G'F(i[L,H]) + i[H,G'(H)]). \tag{6.43}$$

Substituting Eqs. (6.13), (4.5), (2.5), and (1.2) in Eq. (6.43), one has

$$\begin{aligned}C &= FQFi[(P+qQ)(H), P(H)+Q(H)] + Fi[H,Q(H)] \\ &= FQFi\left([P(H),Q(H)] + q[Q(H),P(H)]\right) + Fi\left([P(H)+Q(H),Q(H)]\right) \\ &= FQFi(1-q)[P(H),Q(H)] + Fi[P(H),Q(H)].\end{aligned} \tag{6.44}$$

Equation (6.44) can be rewritten as follows:

$$\begin{aligned}C = F(P+Q)Fi(1-q)[P(H),Q(H)] + Fi[P(H),Q(H)] \\ - FPFi(1-q)[P(H),Q(H)].\end{aligned} \tag{6.45}$$

But using Eq. (1.2) and (2.6) one has

$$PF = P(P + \frac{1}{q}Q) = P^2 = P, \tag{6.46}$$

and using Eq. (6.46), (2.5), and (2.6), then Eq.(6.45) becomes

$$\begin{aligned} C &= F^2((1-q+F^{-1})i[P(H),Q(H)] - F^{-1}Pi(1-q)[P(H),Q(H)]) \\ &= F^2(1-q+P+qQ-P(1-q))i[P(H),Q(H)] \\ &= F^2(1-q+q(P+Q))i[P(H),Q(H)], \end{aligned} \tag{6.47}$$

or using Eq. (1.2), then

$$C = F^2 i[P(H),Q(H)]. \tag{6.48}$$

This is a useful form for the inhomogeneous term in the lifted Jacobi equation, Eq. (6.36) [**1**].

Next combining Eqs.(6.36), (6.43) and (6.48), the lifted Jacobi equation for varying penalty parameter q is then given by

$$\frac{d}{dt}K = i(q-1)F([Q(H),P(K)] - [P(H),Q(K)]) - F^2 i[P(H),Q(H)]. \tag{6.49}$$

In terms of the solution for $K(t)$, the lifted Jacobi field for varying penalty parameter can first be written as

$$J(t) = J(0) + \int_0^t dt' \frac{dJ(t')}{dt'}. \tag{6.50}$$

But according to Eqs. (6.25) and (6.21), one has

$$\frac{dJ(t)}{dt} = U^\dagger(t)K(t)U(t), \tag{6.51}$$

and substituting Eq. (6.51) in Eq. (6.50), one obtains

$$J(t) = J(0) + \int_0^t dt' U^\dagger(t')K(t')U(t'). \tag{6.52}$$

Next consider the case in which the Hamiltonian is constant along a geodesic. The geodesic Eq. (4.4) then implies

$$[G(H),H] = 0. \tag{6.53}$$

Also, using Eqs. (4.10). (2.6), (1.2), (4.5), and (6.13), one has

$$\begin{aligned} 0 = \frac{dH}{dt} &= G^{-1}\frac{dL}{dt} = iF[L,F(L)] = iF[L,P(L)+q^{-1}Q(L)] \\ &= iF[L,P(L)+q^{-1}(1-P)(L))] \\ &= i(1-q^{-1})F[L,P(L)] \\ &= i(1-q^{-1})F[P(H)+qQ(H),P(P(H)+qQ(H)] \\ &= i(1-q^{-1})F[P(H)+qQ(H),P(H)] \\ &= i(q-1)F[Q(H),P(H)] = i(1-q)F[P(H),Q(H)] \\ &= i(1-q)F[H,Q(H)] \\ &= i(1-q)F[H,G'(H)] = 0. \end{aligned} \tag{6.54}$$

It then follows from Eqs. (6.36), (6.53), and (6.54) that if the Hamiltonian is constant, then again one obtains the conventional Jacobi equation, Eq.(6.37). Thus if the Hamiltonian is constant, and $J(0) = 0$ and $dJ(0)/dt = 0$, then in accord with

Eq. (6.86) below, $J(t)$ is proportional to $dJ(0)/dt$ and therefore $J(t) = 0$. In this case it then follows that the geodesics for the lifted Jacobi equation for varying penalty parameter remain the same as for the conventional Jacobi equation and are the same for all values of the penalty parameter q.

The so-called geodesic derivative can be used to determine geodesics which evolve to a chosen unitary transformation U [**1**]. One first chooses a Hamiltonian $H(0)$ which produces $U = \exp(-iH(0)T)$ at some fixed time T along the geodesic for penalty parameter $q = 1$. The parameter q can next be varied to produce a corresponding change in the initial Hamiltonian, and this produces the so-called geodesic derivative $dH_q(0)/dq$. Integration then may produce a geodesic connecting the identity $U(0) = I$ and the chosen unitary transformation $U(T)$ for any penalty parameter q.

To proceed then, the general lifted Jacobi equation, Eq. (6.36), for varied penalty parameter can be solved. [It is convenient to solve Eq. (6.36) directly, instead of Eq. (6.49).] First substituting Eq. (6.43) in Eq. (6.36), one has

$$\frac{d}{dt}K = -i\ F([K, L] + [H, G(K)]) - C. \tag{6.55}$$

The corresponding homogeneous equation is then

$$\frac{d}{dt}K_s = -i\ F([K_s, L] + [H, G(K_s)]), \tag{6.56}$$

and it can be solved if it is first recast in vectorized form [**27**],[**28**]. For any matrix

$$M = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{21} & ... & a_{2n} \\ : & : & ... & : \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix}, \tag{6.57}$$

one defines the vectorized form of the matrix M by the column vector,

$$\text{vec } M = [a_{11}..a_{m1}, a_{12}..a_{m2}...a_{1n}...a_{mn}]^{\mathrm{T}}, \tag{6.58}$$

with each column of the matrix M appearing beneath the previous one, arranged in a column vector. If one has a matrix equation

$$C = AX + XB \tag{6.59}$$

for matrices A, B, C and X, then it can be shown that [**27**],

$$\text{vec } C = \left[(I \otimes A) + (B^{\mathrm{T}} \otimes I)\right] \text{vec } X. \tag{6.60}$$

It then follows that the homogeneous Eq. (6.56) can be written in vectorized form as follows:

$$\begin{aligned} \frac{d}{dt}(\text{vec } K_s) &= -i\text{Fvec } [K_sL - LK_s + HG(K_s) - G(K_s)H] \\ &= i\text{Fvec } [(LK_s + K_s(-L)) - (HG(K_s) + G(K_s)(-H))] \\ &= i\text{F}[(I \otimes L - L^{\mathrm{T}} \otimes I)\text{vec } K_s - (I \otimes H - H^{\mathrm{T}} \otimes I)\text{vec G}(K_s)] \\ &= i\text{F}[[(I \otimes L - L^{\mathrm{T}} \otimes I) + (H^{\mathrm{T}} \otimes I - I \otimes H)\text{G}]\text{vec } (K_s)] \\ &= iA\text{vec } K_s, \end{aligned} \tag{6.61}$$

where

$$A = \text{F}\left[(I \otimes L - L^{\mathrm{T}} \otimes I) + (H^{\mathrm{T}} \otimes I - I \otimes H)\text{G}\right], \tag{6.62}$$

and F and G are the vectorized forms of the superoperators F and G, respectively [**1**]. For example, the superoperator F acting on the matrix X can clearly be written as

$$F(X) = \sum_j A_j X B_j, \tag{6.63}$$

for some matrices A_j and B_j. But one has [**27**]

$$\text{vec } A_j X B_j = (B_j^{\mathrm{T}} \otimes A_j)\text{vec } X, \tag{6.64}$$

and using Eq. (6.64) in Eq. (6.63), then

$$\text{vec } F(X) = \sum_j (B_j^{\mathrm{T}} \otimes A_j)\text{vec } X, \tag{6.65}$$

and therefore the vectorized form F of the superoperator F is given by

$$\mathrm{F} = \sum_j (B_j^{\mathrm{T}} \otimes A_j)\text{vec}. \tag{6.66}$$

Evidently the solution to Eq. (6.61) is

$$\text{vec } K_s(t) = \mathrm{T}\left(\exp\left(i\int_0^t A(t')dt'\right)\right)\text{vec } K_s(0), \tag{6.67}$$

or

$$\text{vec} K_s(t) = \kappa_t \text{vec } K_s(0), \tag{6.68}$$

where

$$\kappa_t = \mathrm{T}\left(\exp\left(i\int_0^t A(t')dt'\right)\right). \tag{6.69}$$

It follows from Eq. (6.69) that

$$\frac{d}{dt}\kappa_t = iA(t)\kappa_t. \tag{6.70}$$

Here κ_t is the propagator for the homogeneous form of Eq. (6.55), namely Eq. (6.56). The solution to Eq. (6.55) is then given by

$$K(t) = \text{unvec}\left(\kappa_t \text{vec } K(0) - \kappa_t \int_0^t dr \kappa_r^{-1} \text{vec } C(r)\right), \tag{6.71}$$

in which unvec unvectorizes [**1**], namely, for a matrix M,

$$\text{unvec } (\text{vec } M) = M. \tag{6.72}$$

To see that Eq. (6.71) solves Eq. (6.55), one has

$$\frac{d}{dt}K(t) = \text{unvec}\left(\frac{d}{dt}\kappa_t \text{vec } K(0) - (\frac{d}{dt}\kappa_t)\int_0^t dr \kappa_r^{-1}\text{vec } C(r) - \kappa_t \kappa_t^{-1}\text{vec } C(t)\right). \tag{6.73}$$

Substituting Eq. (6.70) in Eq. (6.73), then

(6.74)
$$\frac{d}{dt}K(t) = \text{unvec}\left(iA(t)\kappa_t \text{vec } K(0) - iA(t)\kappa_t \int_0^t dr \kappa_t^{-1} \text{vec } C(r) - \text{vec } C(t)\right),$$

and substituting Eq. (6.71) in Eq. (6.74), then

(6.75)
$$\frac{d}{dt}K(t) = \text{unvec}\left(iA(t)\kappa_t \text{vec } K(0) + iA(t)(\text{vec } K(t) - \kappa_t \text{vec } K(0)) - \text{vec } C(t)\right),$$

or

$$\frac{d}{dt}K(t) = \text{unvec}\left(iA(t)\text{vec } K(t) - \text{vec } C(t)\right). \tag{6.76}$$

Substituting Eq. (6.62) in Eq. (6.76), then

(6.77)
$$\frac{d}{dt}K(t) = \text{unvec}\left(i\text{F}\left[(I\otimes L - L^{\text{T}}\otimes I) + (H^{\text{T}}\otimes I - I\otimes H)\text{G}\right]\text{vec}K(t)\right) - C(t).$$

But according to Eqs. (6.56), (6.61), and (6.62),

$$\begin{aligned} &\text{unvec}\left(i\text{F}\left(\left[(I\otimes L - L^{\text{T}}\otimes I) + (H^{\text{T}}\otimes I - I\otimes H)\text{G}\right]\text{vec}K(t)\right)\right) \\ &= -i\ F([K,L] + [H,G(K)]), \end{aligned} \tag{6.78}$$

and then substituting Eq. (6.78) in Eq. (6.77) one obtains Eq. (6.55)

$$\frac{d}{dt}K = -i\ F([K,L] + [H,G(K)] - C, \tag{6.79}$$

as required.

Next, in order to obtain the propagator of the standard (unlifted) Jacobi field J_s, using Eq. (6.64), then Eq. (6.51) in vectorized form is

$$\text{vec}\ (\frac{d}{dt}J_s) = (U^{\text{T}}\otimes U^{\dagger})\text{vec}\ K_s. \tag{6.80}$$

Substituting Eq. (6.68) in Eq. (6.80), then

$$\text{vec}\ (\frac{d}{dt}J_s) = (U^{\text{T}}\otimes U^{\dagger})\kappa_t\text{vec}\ K_s(0). \tag{6.81}$$

Next substituting Eq. (6.51) in Eq. (6.81),

$$\text{vec}\ (\frac{d}{dt}J_s) = (U^{\text{T}}\otimes U^{\dagger})\kappa_t\text{vec}\ (U(0)\frac{d}{dt}J_s(0)U(0)^{\dagger}), \tag{6.82}$$

then for $U(0) = I$, one has

$$\text{vec}\ (\frac{d}{dt}J_s) = (U^{\text{T}}\otimes U^{\dagger})\kappa_t\text{vec}\frac{d}{dt}J_s(0). \tag{6.83}$$

Unvectorizing Eq. (6.83), then

$$\frac{d}{dt}J_s = \text{unvec}\ [(U^{\text{T}}\otimes U^{\dagger})\kappa_t(\text{vec}\frac{d}{dt}J_s(0))]. \tag{6.84}$$

But assuming $J_s(0) = 0$, one has

$$J_s(t) = \int_0^t dt' \frac{d}{dt}J_s(t'), \tag{6.85}$$

and substituting Eq. (6.84) in Eq. (6.85), then

$$J_s(t) = \int_0^t dt' \text{unvec } [(U^{\mathrm{T}} \otimes U^{\dagger})\kappa_{t'}(\text{vec } \frac{d}{dt'} J_s(0))]. \tag{6.86}$$

Next defining the propagator j_T that generates the standard unlifted Jacobi field at time T by

$$J_s(T) = j_T(\frac{d}{dt'} J_s(0)), \tag{6.87}$$

then according to Eq. (6.86), one has

$$j_T = \int_0^T dt' \text{unvec } (U^{\mathrm{T}} \otimes U^{\dagger})\kappa_{t'} \text{vec}. \tag{6.88}$$

It follows from Eqs. (6.71), (6.51), (6.85) and the homogeneous term having the same form as Eq. (6.87) that at time T the solution to the lifted Jacobi equation for varying penalty parameter is given by

$$J(T) = j_T(\frac{d}{dt} J(0)) - \int_0^T dt U(t)^{\dagger} \left(\text{unvec } \kappa_t \left(\int_0^t dr \kappa_r^{-1} \text{vec } C(r) \right) \right) U(t). \tag{6.89}$$

If $J(T) = 0$ in Eq. (6.89), then

$$\frac{d}{dt} J(0) = j_T^{-1} \left[\int_0^T dt U(t)^{\dagger} \left(\text{unvec } \kappa_t \left(\int_0^t dr \kappa_r^{-1} \text{vec } C(r) \right) \right) U(t) \right]. \tag{6.90}$$

Next, according to Eq. (6.6), the Hamiltonian H_q for penalty parameter q is such that

$$\frac{d}{dq} H_q(0) = \frac{d}{dt} J(0), \tag{6.91}$$

and substituting Eq. (6.90) in Eq. (6.91), one obtains the so-called geodesic derivative [**1**]

$$\frac{d}{dq} H_q(0) = j_T^{-1} \left[\int_0^T dt U(t)^{\dagger} \text{unvec} \left(\kappa_t \left(\int_0^t dr \kappa_r^{-1} \text{vec } C(r) \right) \right) U(t) \right]. \tag{6.92}$$

For $q = 1$, one has according to Eqs. (1.2), (2.5) and (2.6),

$$F = P + \frac{1}{q} Q = P + Q = G = 1, \quad q = 1, \tag{6.93}$$

and then according to Eq. (4.4) the Hamiltonian is constant,

$$\frac{dH}{dt} = 0, \quad q = 1. \tag{6.94}$$

Then Eq. (6.48) becomes

$$C = i[P(H), Q(H)], \quad q = 1, \tag{6.95}$$

and then because of Eq. (6.94),

$$\frac{dC}{dt} = 0, \quad q = 1. \tag{6.96}$$

Therefore in Eq. (6.92) for $q = 1$ one has using Eqs. (6.48) and (6.93),

$$Z \equiv \kappa_t \left(\int_0^t dr \kappa_r^{-1} \text{vec } C(r) \right) = \kappa_t \left(\int_0^t dr \kappa_r^{-1} i\text{vec } [P(H), Q(H)] \right), \tag{6.97}$$

and therefore

$$\frac{dZ}{dt} \equiv \left[\frac{d\kappa_t}{dt} \left(\int_0^t dr \kappa_r^{-1} \right) + 1 \right] i\text{vec } [P(H), Q(H)]. \tag{6.98}$$

But for $q = 1$ in Eq. (6.62), one has, according to Eqs. (6.93), (2.5), and (4.5), $F = 1$, $G = 1$, and $L = H$, and therefore

$$A = [I \otimes H - H^{\mathrm{T}} \otimes I + H^{\mathrm{T}} \otimes I - I \otimes H] = 0, \quad q = 1. \tag{6.99}$$

Then substituting Eq. (6.99) in Eq. (6.70), one obtains

$$\frac{d\kappa_t}{dt} = 0. \tag{6.100}$$

Also, according to Eq. (6.69) for $t = 0$, one has

$$\kappa_t = 1. \tag{6.101}$$

Then substituting Eq. (6.100) in Eq. (6.98), one obtains

$$\frac{dZ}{dt} \equiv i\text{vec } [P(H), Q(H)]. \tag{6.102}$$

Also, according to Eqs. (6.97) and (6.101),

$$Z(0) = 0. \tag{6.103}$$

Then combining Eqs. (6.102) and (6.103), one obtains for $q = 1$,

$$Z = it\text{vec } [P(H), Q(H)], \quad q = 1, \tag{6.104}$$

or using Eqs. (6.97) and (6.104), then

$$\kappa_t \left(\int_0^t dr \kappa_r^{-1} \text{vec } C(r) \right) = it\text{vec } [P(H), Q(H)], \quad q = 1. \tag{6.105}$$

Substituting Eq. (6.105) in Eq. (6.92), then for $q = 1$, one has

$$\frac{d}{dq} H_q(0) = j_T^{-1} \left[\int_0^T dt U(t)^\dagger it [P(H), Q(H)] U(t) \right], \quad q = 1. \tag{6.106}$$

For $q \neq 1$, one has, substituting Eq. (6.48) in Eq. (6.92),

$$\frac{d}{dq} H_q(0) = j_T^{-1} \left[\int_0^T dt U(t)^\dagger \text{unvec} \left(\kappa_t \left(\int_0^t dr \kappa_r^{-1} \text{vec } F^2 i [P(H), Q(H)] \right) \right) U(t) \right]. \tag{6.107}$$

Equations (6.106) and (6.107) give the so-called geodesic derivative [**1**] which is useful in the numerical determination of optimal geodesics.

7. Conclusion

In this expository work on the Riemannian geometry of quantum computation, the Riemann curvature, geodesic equation, and lifted Jacobi equation on the manifold of the $SU(2^n)$ group of n-qubit unitary operators with unit determinant were explicitly derived using the Lie algebra $su(2^n)$. The Riemann curvature is given by Eqs. (3.24). The geodesic equation is given by Eqs. (4.10). The generic Jacobi equation and its solution are given by Eqs. (5.22) and (5.58), respectively. The generic lifted Jacobi equation is given by Eqs. (5.37), and the solution is given by Eq. (5.64). The lifted Jacobi equation on the $SU(2^n)$ manifold, for varying penalty parameter, is given by Eq. (6.36) or Eq. (6.49) respectively, and the solution is given by Eqs. (6.71) and (6.48). Also, the geodesic derivative is given by Eq. (6.92). These equations are germane to investigations of conjugate points and the global characteristics of geodesic paths [**6**], [**9**] and minimal complexity quantum circuits [**1**], [**19**], [**2**].

References

[1] M. R. Dowling and M. A. Nielsen, "The Geometry of Quantum Computation," Quantum Information and Computation **8**, 0861-0899 (2008).

[2] H. E. Brandt, "Riemannian Geometry of Quantum Computation," to appear in Nonlinear Analysis (2008).

[3] J. Milnor, "Curvatures of Left Invariant Metrics on Lie Groups," Advances in Mathematics **21**, 293-329 (1976).

[4] V. I. Arnold, *Mathematical Methods of Classical Mechanics*, 2nd Edition, Springer-Verlag, New York (1989).

[5] V. I. Arnold and B. A. Khesin, *Topological Methods in Hydrodynamics*, Springer, New York (1999).

[6] M. Berger, *A Panoramic View of Riemannian Geometry*, Springer-Verlag, Berlin (2003).

[7] A. A. Sagle and R. E. Walde, *Introduction to Lie Groups and Lie Algebras*, Academic Press, New York (1973).

[8] L. Conlon, *Differentiable Manifolds,* 2nd Edition, Birkhäuser, Berlin (2001).

[9] J. M. Lee, *Riemannian Manifolds: An Introduction to Curvature*, Springer, New York (1997).

[10] J. Milnor, *Morse Theory*, Princeton University Press, Princeton, NJ (1973).

[11] B. C. Hall, *Lie Groups, Lie Algebras, and Representations*, Springer, New York (2004).

[12] M. M. Postnikov, *Geometry VI: Riemannian Geometry, Encyclopedia of Mathematical Sciences*, vol. 91, Springer-Verlag, Berlin (2001).

[13] P. Petersen, *Riemannian Geometry*, 2nd Edition, Springer, New York (2006).

[14] M. A. Naimark and A. I. Stern, *Theory of Group Representations,* Springer-Verlag, *New York (1982).*

[15] Mark R. Sepanski, *Compact Lie Groups*, Springer (2007).

[16] Walter Pfeifer, *The Lie Algebras su(N),* Birkhäuser, Basel, (2003).

[17] J. F. Cornwell, *Group Theory in Physics: An Introduction*, Academic Press, San Diego, CA (1997).

[18] J. F. Cornwell, *Group Theory in Physics,* Vols. I and II, Academic Press, London (1984).

[19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[20] C. W. Misner, K. S. Thorne, and J. A. Wheeler, *Gravitation*, pp. 224, 310, W. H. Freeman and Company, New York (1973).

[21] P. D. Lax, "Integrals of Nonlinear Equations of Evolution and Solitary Waves," Communications on Pure and Applied Math. **21**, 467-490 (1968).

[22] E. Zeidler, *Nonlinear Functional Analysis and its Applications IV: Applications to Mathematical Physics*, Springer-Verlag, New York, NY (1997).

[23] D. Zwillinger, *Handbook of Differential Equations,* Third Edition, Academic Press, San Diego, CA (1998).

[24] R. Wasserman, *Tensors and Manifolds,* 2nd Edition, Oxford University Press, Oxford, UK (2004).
[25] W. Greiner and J. Reinhardt, *Field Quantization*, 219, Springer-Verlag, Berlin (1996).
[26] S. Weinberg, *The Quantum Theory of Fields I*, 143, Cambridge University Press (1995).
[27] R. Horn and C. Johnson, *Topics in Matrix Analysis*, 255, Cambridge University Press (1991).
[28] M. A. Nielsen, "A Geometric Approach to Quantum Computation," Quantum Information and Computation **6**, 213-262 (2006).

U.S. Army Research Laboratory, Adelphi, MD, U.S.
E-mail address: hbrandt@arl.army.mil

Contemporary Mathematics
Volume **536**, 2011

A Quantum Model for the Jones Polynomial, Khovanov Homology and Generalized Simplicial Homology

Louis H. Kauffman

ABSTRACT. This paper gives a quantum statistical intpretation of the bracket polynomial, the associated Khovanov homology and a generalization of Khovanov homology in a simplicial categorical context. In this picture the Jones polynomial is replaced by a unitary transformation of the Khovanov chain complex that extends to an action on the homology.

1. Introduction

In this paper we give a quantum statistical interpretation for the bracket polynomial state sum $\langle K \rangle$ and for the Jones polynomial $V_K(t)$. We use this quantum mechanical interpretation to give a new quantum algorithm for computing the Jones polynomial. This algorithm is useful for its conceptual simplicity and it applies to all values of the polynomial variable that lie on the unit circle in the complex plane. Letting $\mathcal{C}(K)$ denote the Hilbert space for this model, there is a natural unitary transformation

$$U : \mathcal{C}(K) \longrightarrow \mathcal{C}(K)$$

such that

$$\langle K \rangle = < \psi | U | \psi >$$

where $|\psi\rangle$ is a sum over basis states for $\mathcal{C}(K)$. The quantum algorithm comes directly from this formula via the Hadamard Test. We then show that the framework for our quantum model for the bracket polynomial is a natural setting for Khovanov homology. The Hilbert space $\mathcal{C}(K)$ of our model has a basis in one-to-one correspondence with the enhanced states of the bracket state summmation and is isomorphic with the chain complex for Khovanov homology with coefficients in the complex numbers. We show that for the Khovanov boundary operator $\partial : \mathcal{C}(K) \longrightarrow \mathcal{C}(K)$, we have the relationship $\partial U + U\partial = 0$. Consequently, the operator U acts on the Khovanov homology, and we therefore obtain a direct relationship between Khovanov homology and this quantum algorithm for the Jones polynomial.

Finally, we show how the Khovanov homology and the Hilbert space context of this paper fit into a simplicial formulation in terms of a functor $\mathcal{F}$ defined on an n-cube category and taking its values in an abelian category. This simplicial description of Khovanov homology lets us make a larger conceptualization of the possible relationship of homology

1991 *Mathematics Subject Classification.* 57M25.

Key words and phrases. bracket polynomial, Khovanov homology, simplicial category, unitary transformation, quantum computing, topological quantum information theory.

and the Hilbert space with its quantum dynamics and measurement. The natural Hilbert space to take in our context is the space whose basis is the set of A, B sequences that form the objects of the n-cube category $\mathcal{D}^n$. We then see that a functor $\mathcal{F} : \mathcal{D}^n \longrightarrow \mathcal{M}$ to a module category $\mathcal{M}$ provides the extra structure of Hilbert space on $\mathcal{C}(\mathcal{F})$ that supports the homology $H_\star\mathcal{C}(\mathcal{F})$. In the case of Khovanov homology, this extra structure amounts to the enhancements of the standard bracket states. The standard bracket states are in 1-1 correspondence with the sequences in $\mathcal{D}^n$ and so we have a very concrete description of this functorial relationship. More generally, the categorical picture shows how a basic Hilbert space is boosted to acquire new elements and extra structure that allow it to support non-trivial homology and unitary transformations that respect that homology. There is much work to be done in exploring this relationship of quantum information and algebraic topology.

This paper is a modification and extension of [**14**]. The paper is organized as follows. Section 2 reviews the structure of the bracket polynomial, its state summation, the use of enhanced states and the relationship with the Jones polynomial. Section 3 describes the quantum statistical model for the bracket polynomial and refers to Section 8 (the Appendix) for the details of the Hadamard test and the structure of the quantum algorithm. Section 4 describes the relationship of the quantum model with Khovanov homology axiomatically, without using the specific details of the Khovanov chain complex that give these axioms. Section 5 discusses possible extensions of the method of this paper. In particular, we raise the question of finding other unitary actions on Khovanov Homology. In Section 6 we construct the Khovanov chain complex in detail and show how some of its properties follow uniquely from the axioms of the previous section. Section 7 discusses the simplicial and functorial structure described above. In Section 8 (the Appendix) we detail the Hadamard test.

Acknowledgement. It gives the author great pleasure to thank A. K. Bousfield for useful conversations about simplicial structures in relation to Khovanov homology.

2. Bracket Polynomial and Jones Polynomial

The bracket polynomial [**11**] model for the Jones polynomial [**8, 9, 10, 31**] is usually described by the expansion

$$\langle \times \rangle = A\langle)(\rangle + A^{-1}\langle) (\rangle$$

Here the small diagrams indicate parts of otherwise identical larger knot or link diagrams. The two types of smoothing (local diagram with no crossing) in this formula are said to be of type A (A above) and type B (A^{-1} above).

$$\langle \bigcirc \rangle = -A^2 - A^{-2}$$
$$\langle K \bigcirc \rangle = (-A^2 - A^{-2})\langle K \rangle$$
$$\langle \, \backslash / \, \rangle = (-A^3)\langle \smile \rangle$$
$$\langle \, \backslash \bigcirc / \, \rangle = (-A^{-3})\langle \smile \rangle$$

One uses these equations to normalize the invariant and make a model of the Jones polynomial. In the normalized version we define

$$f_K(A) = (-A^3)^{-wr(K)}\langle K \rangle / \langle \bigcirc \rangle$$

where the writhe $wr(K)$ is the sum of the oriented crossing signs for a choice of orientation of the link K. Since we shall not use oriented links in this paper, we refer the reader to [**11**] for the details about the writhe. One then has that $f_K(A)$ is invariant under the Reidemeister moves (again see [**11**]) and the original Jones polynonmial $V_K(t)$ is given by the formula

$$V_K(t) = f_K(t^{-1/4}).$$

The Jones polynomial has been of great interest since its discovery in 1983 due to its relationships with statistical mechanics, due to its ability to often detect the difference between a knot and its mirror image and due to the many open problems and relationships of this invariant with other aspects of low dimensional topology.

The State Summation. In order to obtain a closed formula for the bracket, we now describe it as a state summation. Let K be any unoriented link diagram. Define a *state*, S, of K to be the collection of planar loops resulting from a choice of smoothing for each crossing of K. There are two choices (A and B) for smoothing a given crossing, and thus there are $2^{c(K)}$ states of a diagram with $c(K)$ crossings. In a state we label each smoothing with A or A^{-1} according to the convention indicated by the expansion formula for the bracket. These labels are the *vertex weights* of the state. There are two evaluations related to a state. The first is the product of the vertex weights, denoted $\langle K|S\rangle$. The second is the number of loops in the state S, denoted $||S||$.
Define the *state summation*, $\langle K\rangle$, by the formula

$$\langle K\rangle = \sum_S < K|S > \delta^{||S||}$$

where $\delta = -A^2 - A^{-2}$. This is the state expansion of the bracket. It is possible to rewrite this expansion in other ways. For our purposes in this paper it is more convenient to think of the loop evaluation as a sum of *two* loop evaluations, one giving $-A^2$ and one giving $-A^{-2}$. This can be accomplished by letting each state curve carry an extra label of $+1$ or -1. We describe these *enhanced states* below.

Changing Variables. Letting $c(K)$ denote the number of crossings in the diagram K, if we replace $\langle K\rangle$ by $A^{-c(K)}\langle K\rangle$, and then replace A^2 by $-q^{-1}$, the bracket is then rewritten in the following form:

with $\langle \bigcirc \rangle = (q + q^{-1})$. It is useful to use this form of the bracket state sum for the sake of the grading in the Khovanov homology (to be described below). We shall continue to refer to the smoothings labeled q (or A^{-1} in the original bracket formulation) as B*-smoothings*.

Using Enhanced States. We now use the convention of *enhanced states* where an enhanced state has a label of 1 or -1 on each of its component loops. We then regard the value of the loop $q+q^{-1}$ as the sum of the value of a circle labeled with a 1 (the value is q) added to the value of a circle labeled with an -1 (the value is q^{-1}). We could have chosen the less neutral labels of $+1$ and X so that

$$q^{+1} \Longleftrightarrow +1 \Longleftrightarrow 1$$

and

$$q^{-1} \Longleftrightarrow -1 \Longleftrightarrow X,$$

since an algebra involving 1 and X naturally appears later in relation to Khovanov homology. It does no harm to take this form of labeling from the beginning. The use of enhanced states for formulating Khovanov homology was pointed out by Oleg Viro in [**30**].

Consider the form of the expansion of this version of the bracket polynonmial in enhanced states. We have the formula as a sum over enhanced states s :

$$\langle K \rangle = \sum_s (-1)^{i(s)} q^{j(s)}$$

where $i(s)$ is the number of B-type smoothings in s and $j(s) = i(s) + \lambda(s)$, with $\lambda(s)$ the number of loops labeled 1 minus the number of loops labeled -1 in the enhanced state s.

One advantage of the expression of the bracket polynomial via enhanced states is that it is now a sum of monomials. We shall make use of this property throughout the rest of the paper.

3. Quantum Statistics and the Jones Polynomial

We now use the enhanced state summation for the bracket polynomial with variable q to give a quantum formulation of the state sum. Let q be on the unit circle in the complex plane. (This is equivalent to letting the original bracket variable A be on the unit circle and equivalent to letting the Jones polynmial variable t be on the unit circle.) Let $\mathcal{C}(K)$ denote the complex vector space with orthonormal basis $\{|s\rangle\}$ where s runs over the enhanced states of the diagram K. The vector space $\mathcal{C}(K)$ is the (finite dimensional) Hilbert space for our quantum formulation of the Jones polynomial. While it is customary for a Hilbert space to be written with the letter H, we do not follow that convention here, due to the fact that we shall soon regard $\mathcal{C}(K)$ as a chain complex and take its homology. One can hardly avoid using $\mathcal{H}$ for homology.

With q on the unit circle, we define a unitary transformation

$$U : \mathcal{C}(K) \longrightarrow \mathcal{C}(K)$$

by the formula

$$U|s\rangle = (-1)^{i(s)} q^{j(s)} |s\rangle$$

for each enhanced state s. Here $i(s)$ and $j(s)$ are as defined in the previous section of this paper.

Let

$$|\psi\rangle = \sum_s |s\rangle.$$

The state vector $|\psi\rangle$ is the sum over the basis states of our Hilbert space $\mathcal{C}(K)$. For convenience, we do not normalize $|\psi\rangle$ to length one in the Hilbert space $\mathcal{C}(K)$. We then have the

Lemma. The evaluation of the bracket polynomial is given by the following formula

$$\langle K \rangle = \langle \psi | U | \psi \rangle.$$

Proof.

$$\langle\psi|U|\psi\rangle = \sum_{s'}\sum_{s}\langle s'|(-1)^{i(s)}q^{j(s)}|s\rangle = \sum_{s'}\sum_{s}(-1)^{i(s)}q^{j(s)}\langle s'|s\rangle$$

$$= \sum_{s}(-1)^{i(s)}q^{j(s)} = \langle K\rangle,$$

since

$$\langle s'|s\rangle = \delta(s,s')$$

where $\delta(s,s')$ is the Kronecker delta, equal to 1 when $s = s'$ and equal to 0 otherwise. //

Thus the bracket polyomial evaluation is a quantum amplitude for the measurement of the state $U|\psi\rangle$ in the $\langle\psi|$ direction. Since $\langle\psi|U|\psi\rangle$ can be regarded as a diagonal element of the transformation U with respect to a basis containing $|\psi\rangle$, this formula can be taken as the foundation for a quantum algorithm that computes the bracket of K via the Hadamard test. See the Appendix to this paper, for a discussion of the Hadamard test and the corresponding quantum algorithm.

A few words about quantum algorithms are appropropiate at this point. In general one begins with an intial state $|\psi\rangle$ and a unitary transformation U. Quantum processes are modeled by unitary transformations, and it is in principle possible to create a physical process corresponding to any given unitary transformation. In practice, one is limited by the dimensions of the spaces involved and by the fact that physical quantum states are very delicate and subject to decoherence. Nevertheless, one designs quantum algorithms at first by finding unitary operators that represent the informaton in the problem one wishes to calculate. Then the quantum part of the quantum computation is the physical process that produces the state $U|\psi\rangle$ from the initial state $|\psi\rangle$. At this point $U|\psi\rangle$ is available for measurement. Interaction with the environment is effectively a measurement, and will happen in any case, but one intends a controlled circumstance in which the measurement can occur. If $\{|e_1\rangle, \cdots |e_n\rangle\}$ is a basis for the Hilbert space (here denoted by $\mathcal{C}(K)$) then we would have

$$U|\psi\rangle = \sum_{k} z_k|e_k\rangle,$$

a linear combination of the basis elements. On measuring with respect to this basis, each $|e_k\rangle$ corresponds to an observable outcome and *this outcome will occur with frequency* $|z_k|^2/(\sum_i |z_i|^2)$. The form of quantum computation consists in repeatedly preparing and running the process to find the frequency with which certain key observations occur. In the case of our algorithm we are interested in the frequency of measuring $|\psi\rangle$ as it occurs in $U|\psi\rangle$. This frequency is equal to the absolute square of the inner product $\langle\psi|U|\psi\rangle$. Thus direct measurement of $U|\psi\rangle$ will not give us the value of the inner product itself. For this reason we use the more refined Hadamard test as described in the Appendix. There is much more to be said about quantum algorithms in general and about quantum algorithms for the Jones polynomial in particular. The reader can examine [**1, 15, 16, 17, 28**] for more information.

It is useful to formalize the bracket evaluation as a quantum amplitude. This is a direct way to give a physical interpretation of the bracket state sum and the Jones polynomial. Just how this process can be implemented physically depends upon the interpretation of the Hilbert space $\mathcal{C}(K)$. It is common practice in theorizing about quantum computing and quantum information to define a Hilbert space in terms of some mathematically convenient

basis (such as the enhanced states of the knot or link diagram K) and leave open the possibility of a realization of the space and the quantum evolution operators that have been defined upon it. In principle any finite dimensional unitary operator can be realized by some physical system. In practice, this is the problem of constructing quantum computers and quantum information devices. It is not so easy to construct what can be done in principle, and the quantum states that are produced may be all too short-lived to produce reliable computation. Nevertheless, one has the freedom to create spaces and operators on the mathematical level and to conceptualize these in a quantum mechanical framework. The resulting structures may be realized in nature and in present or future technology. In the case of our Hilbert space associated with the bracket state sum and its corresponding unitary transformation U, there is rich extra structure related to Khovanov homology that we discuss in the next section. One hopes that in a (future) realization of these spaces and operators, the Khovanov homology will play a key role in quantum information related to the knot or link K.

There are a number of conclusions that we can draw from the formula $\langle K \rangle = \langle \psi | U | \psi \rangle$. First of all, this formulation constitutes a quantum algorithm for the computation of the bracket polynomial (and hence the Jones polynomial) at any specialization where the variable is on the unit circle. We have defined a unitary transformation U and then shown that the bracket is an evaluation in the form $\langle \psi | U | \psi \rangle$. This evaluation can be computed via the Hadamard test [**26**] and this gives the desired quantum algorithm. Once the unitary transformation is given as a physical construction, the algorithm will be as efficient as any application of the Hadamard test. The present algorithm requires an exponentially increasing complexity of construction for the associated unitary transformation, since the dimension of the Hilbert space is equal to the $2^{e(K)}$ where $e(K)$ is the number of enhanced states of the diagram K. (Note that $e(K) = \sum_S 2^{||S||}$ where S runs over the $2^{c(K)}$ standard bracket states, $c(K)$ is the number of crossings in the diagram and $||S||$ is the number of loops in the state S.) Nevertheless, it is significant that the Jones polynomial can be formulated in such a direct way in terms of a quantum algorithm. By the same token, we can take the basic result of Khovanov homology that says that the bracket is a graded Euler characteristic of the Khovanov homology as telling us that we are taking a step in the direction of a quantum algorithm for the Khovanov homology itself. This will be discussed below.

4. Khovanov Homology and a Quantum Model for the Jones Polynomial

In this section we outline how the Khovanov homology is related with our quantum model. This can be done essentially axiomatically, without giving the details of the Khovanov construction. We give these details in the next section. The outline is as follows:

(1) There is a boundary operator ∂ defined on the Hilbert space of enhanced states of a link diagram K

$$\partial : \mathcal{C}(K) \longrightarrow \mathcal{C}(K)$$

such that $\partial\partial = 0$ and so that if $\mathcal{C}^{i,j} = \mathcal{C}^{i,j}(K)$ denotes the subspace of $\mathcal{C}(K)$ spanned by enhanced states $|s\rangle$ with $i = i(s)$ and $j = j(s)$, then

$$\partial : \mathcal{C}^{ij} \longrightarrow \mathcal{C}^{i+1,j}.$$

That is, we have the formulas

$$i(\partial|s\rangle) = i(|s\rangle) + 1$$

and

$$j(\partial|s\rangle) = j(|s\rangle)$$

for each enhanced state s. In the next section, we shall explain how the boundary operator is constructed.

(2) **Lemma.** By defining $U : \mathcal{C}(K) \longrightarrow \mathcal{C}(K)$ as in the previous section, via

$$U|s\rangle = (-1)^{i(s)} q^{j(s)} |s\rangle,$$

we have the following basic relationship between U and the boundary operator ∂ :

$$U\partial + \partial U = 0.$$

Proof. This follows at once from the definition of U and the fact that ∂ preserves j and increases i to $i + 1$. //

(3) From this Lemma we conclude that the operator U acts on the homology of $\mathcal{C}(K)$. We can regard $H(\mathcal{C}(K)) = Ker(\partial)/Image(\partial)$ as a new Hilbert space on which the unitary operator U acts. In this way, the Khovanov homology and its relationship with the Jones polynomial has a natural quantum context.

(4) For a fixed value of j,

$$\mathcal{C}^{\bullet,j} = \oplus_i \mathcal{C}^{i,j}$$

is a subcomplex of $\mathcal{C}(K)$ with the boundary operator ∂. Consequently, we can speak of the homology $H(\mathcal{C}^{\bullet,j})$. Note that the dimension of $\mathcal{C}^{ij}$ is equal to the number of enhanced states $|s\rangle$ with $i = i(s)$ and $j = j(s)$. Consequently, we have

$$\langle K \rangle = \sum_s q^{j(s)} (-1)^{i(s)} = \sum_j q^j \sum_i (-1)^i dim(\mathcal{C}^{ij})$$

$$= \sum_j q^j \chi(\mathcal{C}^{\bullet,j}) = \sum_j q^j \chi(H(\mathcal{C}^{\bullet,j})).$$

Here we use the definition of the *Euler characteristic of a chain complex*

$$\chi(\mathcal{C}^{\bullet,j}) = \sum_i (-1)^i dim(\mathcal{C}^{ij})$$

and the fact that the Euler characteristic of the complex is equal to the Euler characteristic of its homology. The quantum amplitude associated with the operator U is given in terms of the Euler characteristics of the Khovanov homology of the link K.

$$\langle K \rangle = \langle \psi | U | \psi \rangle = \sum_j q^j \chi(H(\mathcal{C}^{\bullet,j}(K))).$$

Our reformulation of the bracket polynomial in terms of the unitary operator U leads to a new viewpoint on the Khovanov homology as a representation space for the action of U. The bracket polynomial is then a quantum amplitude that expresses the Euler characteristics of the homology associated with this action. The decomposition of the chain complex into the parts $\mathcal{C}^{i,j}(K)$ corresponds to the eigenspace decomposition of the operator U. The reader will note that in this case the operator U is already diagonal in the basis of enhanced states for the chain complex $\mathcal{C}(K)$. We regard this reformulation as a guide to further questions about the relationship of the Khovanov homology with quantum information associated with the link K.

As we shall see in the next section, the internal combinatorial structure of the set of enhanced states for the bracket summation leads to the Khovanov homology theory, whose graded Euler characteristic yields the bracket state sum. Thus we have a quantum statistical interpretation of the Euler characteristics of the Khovanov homology theory, and a conceptual puzzle about the nature of this relationship with the Hilbert space of that quantum theory. It is that relationship that is the subject of this paper. The unusual point about the Hilbert space is that each of its basis elements has a specific combinatorial structure that is related to the topology of the knot K. Thus this Hilbert space is, from the point of view of its basis elements, a form of "taking apart" of the topological structure of the knot that we are interested in studying.

Homological structure of the unitary transformation. We now prove a general result about the structure of a chain complex that is also a finite dimensional Hilbert space. Let $\mathcal{C}$ be a chain complex over the complex numbers with boundary operator

$$\partial : \mathcal{C}^i \longrightarrow \mathcal{C}^{i+1},$$

with $\mathcal{C}$ denoting the direct sum of all the $\mathcal{C}^i$, $i = 0, 1, 2, \cdots n$ (for some n). Let

$$U : \mathcal{C} \longrightarrow \mathcal{C}$$

be a unitary operator that satisfies the equation $U\partial + \partial U = 0$. We do not assume a second grading j as occurs in the Khovanov homology. However, since U is unitary, it follows [**23**] that there is a basis for $\mathcal{C}$ in which U is diagonal. Let $\mathcal{B} = \{|s\rangle\}$ denote this basis. Let λ_s denote the eigenvalue of U corresponding to $|s\rangle$ so that $U|s\rangle = \lambda_s|s\rangle$. Let $\alpha_{s,s'}$ be the matrix element for ∂ so that

$$\partial|s\rangle = \sum_{s'} \alpha_{s,s'}|s'\rangle$$

where s' runs over a set of basis elements so that $i(s') = i(s) + 1$.

Lemma. With the above conventions, we have that for $|s'\rangle$ a basis element such that $\alpha_{s,s'} \neq 0$ then $\lambda_{s'} = -\lambda_s$.

Proof. Note that

$$U\partial|s\rangle = U(\sum_{s'} \alpha_{s,s'}|s'\rangle) = \sum_{s'} \alpha_{s,s'}\lambda_{s'}|s'\rangle$$

while

$$\partial U|s\rangle = \partial\lambda_s|s\rangle = \sum_{s'} \alpha_{s,s'}\lambda_s|s'\rangle.$$

Since $U\partial + \partial U = 0$, the conclusion of the Lemma follows from the independence of the elements in the basis for the Hilbert space. //

In this way we see that eigenvalues will propagate forward from $\mathcal{C}^0$ with alternating signs according to the appearance of successive basis elements in the boundary formulas for the chain complex. Various states of affairs are possible in general, with new eigenvaluues starting at some $\mathcal{C}^k$ for $k > 0$. The simplest state of affairs would be if all the possible eigenvalues (up to multiplication by -1) for U occurred in $\mathcal{C}^0$ so that

$$\mathcal{C}^0 = \oplus_\lambda \mathcal{C}^0_\lambda$$

where λ runs over all the distinct eigenvalues of U restricted to $\mathcal{C}^0$, and $\mathcal{C}^0_\lambda$ is spanned by all $|s\rangle$ in $\mathcal{C}^0$ with $U|s\rangle = \lambda|s\rangle$. Let us take the further assumption that for each λ as above, the subcomplexes

$$\mathcal{C}^\bullet_\lambda : \mathcal{C}^0_\lambda \longrightarrow \mathcal{C}^1_{-\lambda} \longrightarrow \mathcal{C}^2_{+\lambda} \longrightarrow \cdots \mathcal{C}^n_{(-1)^n\lambda}$$

have $\mathcal{C} = \oplus_\lambda \mathcal{C}^\bullet_\lambda$ as their direct sum. With this assumption about the chain complex, define $|\psi\rangle = \sum_s |s\rangle$ as before, with $|s\rangle$ running over the whole basis for $\mathcal{C}$. Then it follows just as in the beginning of this section that

$$\langle\psi|U|\psi\rangle = \sum_\lambda \lambda\chi(H(C^\bullet_\lambda)).$$

Here χ denotes the Euler characteristic of the homology. The point is, that this formula for $\langle\psi|U|\psi\rangle$ takes exactly the form we had for the special case of Khovanov homology (with eigenvalues $(-1)^i q^j$), but here the formula occurs just in terms of the eigenspace decomposition of the unitary transformation U in relation to the chain complex. Clearly there is more work to be done here and we will return to it in a subsequent paper.

Remark on the density matrix. Given the state $|\psi\rangle$, we can define the *density matrix*

$$\rho = |\psi\rangle\langle\psi|.$$

With this definition it is immediate that

$$Tr(U\rho) = \langle\psi|U|\psi\rangle$$

where $Tr(M)$ denotes the trace of a matrix M. Thus we can restate the form of our result about Euler characteristics as

$$Tr(U\rho) = \sum_\lambda \lambda\chi(H(C^\bullet_\lambda)).$$

In searching for an interpretation of the Khovanov complex in this quantum context it is useful to use this reformulation. For the bracket we have

$$\langle K\rangle = <\psi|U|\psi> = Tr(U\rho).$$

The Hilbert space for expressing the bracket polynomial as a quantum statistical amplitude is quite naturally the chain complex for Khovanov homology with complex coefficients, and the unitary transformation that is the structure of the bracket polynomial acts on the homology of this chain complex. This means that the homology classes contain information preserved by the quantum process that underlies the bracket polynomial. We would like to exploit this direct relationship between the quantum model and the Khovanov homology to obtain deeper information about the relationship of topology and quantum information theory, and we would like to use this relationship to probe the properties of these topological invariants.

5. Discussion and Speculation

The formalism that we have pursued in this paper to relate Khovanov homology and the Jones polynomial with quantum statistics can be generalized to apply to other situations. It is possible to associate a finite dimensional Hilbert space that is also a chain complex (or cochain complex) to topological structures other than knots and links. To formulate this, let X denote the topological structure and $\mathcal{C}(X)$ denote the associated linear space endowed with a boundary operator $\partial : \mathcal{C}(X) \longrightarrow \mathcal{C}(X)$, with $\partial\partial = 0$. We want to consider situations where there is a unitary operator $U : \mathcal{C}(X) \longrightarrow \mathcal{C}(X)$ such that $U\partial + \partial U = 0$ so that U induces a unitary action on $\mathcal{H}(X)$, the homology of $\mathcal{C}(X)$ with respect to ∂.

Even in the case of Khovanov homology, we could keep the homology theory fixed and ask for other unitary operators U that satisfy $U\partial + \partial U = 0$. Knowing other examples of such operators would shed light on the nature of Khovanov homology from the point of view of quantum statistics.

Furthermore, we are concerned with the pattern of the amplitude

$$\langle K \rangle =< \psi|U|\psi >= Tr(U\rho) = \sum_{\lambda} \lambda \chi(H(C^{\bullet}_{\lambda})),$$

where the bracket polynomial or the Jones polynomial is replaced by the unitary transformation U on the Hilbert space and its spectrum of eigenvalues. The question is whether this formulation can be regarded as a useful clue in seeing the nature of the categorification of the Jones polynomial. Instead of categorifying a knot polynomial we are probing a unitary transformation on a Hilbert space with extra structure that makes it a chain complex.

6. Background on Khovanov Homology

In this section, we describe Khovanov homology along the lines of [**20, 2**], and we tell the story so that the gradings and the structure of the differential emerge in a natural way. This approach to motivating the Khovanov homology uses elements of Khovanov's original approach, Viro's use of enhanced states for the bracket polynomial [**30**], and Bar-Natan's emphasis on tangle cobordisms [**3**]. We use similar considerations in our paper [**18**].

Two key motivating ideas are involved in finding the Khovanov invariant. First of all, one would like to *categorify* a link polynomial such as $\langle K \rangle$. There are many meanings to the term categorify, but here the quest is to find a way to express the link polynomial as a *graded Euler characteristic* $\langle K \rangle = \chi_q \langle \mathcal{H}(K) \rangle$ for some homology theory associated with $\langle K \rangle$.

We will use the bracket polynomial and its enhanced states as described in the previous sections of this paper. To see how the Khovanov grading arises, consider the form of the expansion of this version of the bracket polynomial in enhanced states. We have the formula as a sum over enhanced states s :

$$\langle K \rangle = \sum_{s} (-1)^{i(s)} q^{j(s)}$$

where $i(s)$ is the number of B-type smoothings in s, $\lambda(s)$ is the number of loops in s labeled 1 minus the number of loops labeled X, and $j(s) = i(s) + \lambda(s)$. This can be rewritten in the following form:

$$\langle K \rangle = \sum_{i\,,j} (-1)^i q^j dim(\mathcal{C}^{ij})$$

where we define $\mathcal{C}^{ij}$ to be the linear span (over the complex numbers for the purpose of this paper, but over the integers or the integers modulo two for other contexts) of the set of enhanced states with $i(s) = i$ and $j(s) = j$. Then the number of such states is the dimension $dim(\mathcal{C}^{ij})$.

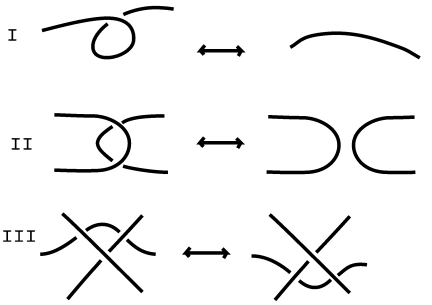


FIGURE 1. **Reidemeister Moves**

We would like to have a bigraded complex composed of the $\mathcal{C}^{ij}$ with a differential

$$\partial : \mathcal{C}^{ij} \longrightarrow \mathcal{C}^{i+1\,j}.$$

The differential should increase the *homological grading* i by 1 and preserve the *quantum grading* j. Then we could write

$$\langle K \rangle = \sum_j q^j \sum_i (-1)^i dim(\mathcal{C}^{ij}) = \sum_j q^j \chi(\mathcal{C}^{\bullet\, j}),$$

where $\chi(\mathcal{C}^{\bullet\, j})$ is the Euler characteristic of the subcomplex $\mathcal{C}^{\bullet\, j}$ for a fixed value of j.

This formula would constitute a categorification of the bracket polynomial. Below, we shall see how *the original Khovanov differential ∂ is uniquely determined by the restriction that $j(\partial s) = j(s)$ for each enhanced state s.* Since j is preserved by the differential, these subcomplexes $\mathcal{C}^{\bullet\, j}$ have their own Euler characteristics and homology. We have

$$\chi(H(\mathcal{C}^{\bullet\, j})) = \chi(\mathcal{C}^{\bullet\, j})$$

where $H(\mathcal{C}^{\bullet\, j})$ denotes the homology of the complex $\mathcal{C}^{\bullet\, j}$. We can write

$$\langle K \rangle = \sum_j q^j \chi(H(\mathcal{C}^{\bullet\, j})).$$

The last formula expresses the bracket polynomial as a *graded Euler characteristic* of a homology theory associated with the enhanced states of the bracket state summation. This is the categorification of the bracket polynomial. Khovanov proves that this homology theory is an invariant of knots and links (via the Reidemeister moves of Figure 1), creating a new and stronger invariant than the original Jones polynomial.

We will construct the differential in this complex first for mod-2 coefficients. The differential is based on regarding two states as *adjacent* if one differs from the other by a single smoothing at some site. Thus if (s, τ) denotes a pair consisting in an enhanced state s and site τ of that state with τ of type A, then we consider all enhanced states s' obtained from s by smoothing at τ and relabeling only those loops that are affected by the resmoothing. Call this set of enhanced states $S'[s, \tau]$. Then we shall define the *partial differential* $\partial_\tau(s)$ as a sum over certain elements in $S'[s, \tau]$, and the differential by the formula

$$\partial(s) = \sum_\tau \partial_\tau(s)$$

with the sum over all type A sites τ in s. It then remains to see what are the possibilities for $\partial_\tau(s)$ so that $j(s)$ is preserved.

Note that if $s' \in S'[s,\tau]$, then $i(s') = i(s) + 1$. Thus

$$j(s') = i(s') + \lambda(s') = 1 + i(s) + \lambda(s').$$

From this we conclude that $j(s) = j(s')$ if and only if $\lambda(s') = \lambda(s) - 1$. Recall that

$$\lambda(s) = [s:+] - [s:-]$$

where $[s:+]$ is the number of loops in s labeled $+1$, $[s:-]$ is the number of loops labeled -1 (same as labeled with X) and $j(s) = i(s) + \lambda(s)$.

Proposition. The partial differentials $\partial_\tau(s)$ are uniquely determined by the condition that $j(s') = j(s)$ for all s' involved in the action of the partial differential on the enhanced state s. This unique form of the partial differential can be described by the following structures of multiplication and comultiplication on the algebra for integral coefficients.

(1) The element 1 is a multiplicative unit and $X^2 = 0$.
(2) $\Delta(1) = 1 \otimes X + X \otimes 1$ and $\Delta(X) = X \otimes X$.

These rules describe the local relabeling process for loops in a state. Multiplication corresponds to the case where two loops merge to a single loop, while comultiplication corresponds to the case where one loop bifurcates into two loops.

Proof. Using the above description of the differential, suppose that there are two loops at τ that merge in the smoothing. If both loops are labeled 1 in s then the local contribution to $\lambda(s)$ is 2. Let s' denote a smoothing in $S[s,\tau]$. In order for the local λ contribution to become 1, we see that the merged loop must be labeled 1. Similarly if the two loops are labeled 1 and X, then the merged loop must be labeled X so that the local contribution for λ goes from 0 to -1. Finally, if the two loops are labeled X and X, then there is no label available for a single loop that will give -3, so we define ∂ to be zero in this case. We can summarize the result by saying that there is a multiplicative structure m such that $m(1,1) = 1, m(1,X) = m(X,1) = x, m(X,X) = 0$, and this multiplication describes the structure of the partial differential when two loops merge. Since this is the multiplicative structure of the algebra $\mathcal{A} = k[X]/(X^2)$, we take this algebra as summarizing the differential.

Now consider the case where s has a single loop at the site τ. Smoothing produces two loops. If the single loop is labeled X, then we must label each of the two loops by X in order to make λ decrease by 1. If the single loop is labeled 1, then we can label the two loops by X and 1 in either order. In this second case we take the partial differential of s to be the sum of these two labeled states. This structure can be described by taking a coproduct structure with $\Delta(X) = X \otimes X$ and $\Delta(1) = 1 \otimes X + X \otimes 1$. We now have the algebra $\mathcal{A} = k[X]/(X^2)$ with product $m : \mathcal{A} \otimes \mathcal{A} \longrightarrow \mathcal{A}$ and coproduct $\Delta : \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A}$, describing the differential completely. This completes the proof. //

Partial differentials are defined on each enhanced state s and a site τ of type A in that state. We consider states obtained from the given state by smoothing the given site τ. The result of smoothing τ is to produce a new state s' with one more site of type B than s. Forming s' from s we either amalgamate two loops to a single loop at τ, or we divide a loop at τ into two distinct loops. In the case of amalgamation, the new state s acquires the label on the amalgamated circle that is the product of the labels on the two circles that

are its ancestors in s. This case of the partial differential is described by the multiplication in the algebra. If one circle becomes two circles, then we apply the coproduct. Thus if the circle is labeled X, then the resultant two circles are each labeled X corresponding to $\Delta(X) = X \otimes X$. If the orginal circle is labeled 1 then we take the partial boundary to be a sum of two enhanced states with labels 1 and X in one case, and labels X and 1 in the other case, on the respective circles. This corresponds to $\Delta(1) = 1 \otimes X + X \otimes 1$. Modulo two, the boundary of an enhanced state is the sum, over all sites of type A in the state, of the partial boundaries at these sites. It is not hard to verify directly that the square of the boundary mapping is zero (this is the identity of mixed partials!) and that it behaves as advertised, keeping $j(s)$ constant. There is more to say about the nature of this construction with respect to Frobenius algebras and tangle cobordisms. In Figures 2,3 and 4 we illustrate how the partial boundaries can be conceptualized in terms of surface cobordisms. The equality of mixed partials corresponds to topological equivalence of the corresponding surface cobordisms, and to the relationships between Frobenius algebras and the surface cobordism category. In particular, in Figure 4 we show how in a key case of two sites (labeled 1 and 2 in that Figure) the two orders of partial boundary are

$$\partial_2 \partial_1 = (1 \otimes m) \circ (\Delta \otimes 1)$$

and

$$\partial_1 \partial_2 = \Delta \circ m.$$

In the Frobenius algebra $\mathcal{A} = k[X]/(X^2)$ we have the identity

$$(1 \otimes m) \circ (\Delta \otimes 1) = \Delta \circ m.$$

Thus the Frobenius algebra implies the identity of the mixed partials. Furthermore, in Figure 3 we see that this identity corresponds to the topological equivalence of cobordisms under an exchange of saddle points. There is more to say about all of this, but we will stop here. The proof of invariance of Khovanov homology with respect to the Reidemeister moves (respecting grading changes) will not be given here. See [**20, 2, 3**]. It is remarkable that this version of Khovanov homology is uniquely specified by natural ideas about adjacency of states in the bracket polynomial.

Remark on Integral Differentials. Choose an ordering for the crossings in the link diagram K and denote them by $1, 2, \cdots n$. Let s be any enhanced state of K and let $\partial_i(s)$ denote the chain obtained from s by applying a partial boundary at the i-th site of s. If the i-th site is a smoothing of type A^{-1}, then $\partial_i(s) = 0$. If the i-th site is a smoothing of type A, then $\partial_i(s)$ is given by the rules discussed above (with the same signs). The compatibility conditions that we have discussed show that partials commute in the sense that $\partial_i(\partial_j(s)) = \partial_j(\partial_i(s))$ for all i and j. One then defines signed boundary formulas in the usual way of algebraic topology. One way to think of this regards the complex as the analogue of a complex in de Rahm cohomology. Let $\{dx_1, dx_2, \cdots, dx_n\}$ be a formal basis for a Grassmann algebra so that $dx_i \wedge dx_j = -dx_j \wedge dx_i$ Starting with enhanced states s in $C^0(K)$ (that is, states with all A-type smoothings) define formally, $d_i(s) = \partial_i(s) dx_i$ and regard $d_i(s)$ as identical with $\partial_i(s)$ as we have previously regarded it in $C^1(K)$. In general, given an enhanced state s in $C^k(K)$ with B-smoothings at locations $i_1 < i_2 < \cdots < i_k$, we represent this chain as $s\, dx_{i_1} \wedge \cdots \wedge dx_{i_k}$ and define

$$\partial(s\, dx_{i_1} \wedge \cdots \wedge dx_{i_k}) = \sum_{j=1}^{n} \partial_j(s)\, dx_j \wedge dx_{i_1} \wedge \cdots \wedge dx_{i_k},$$

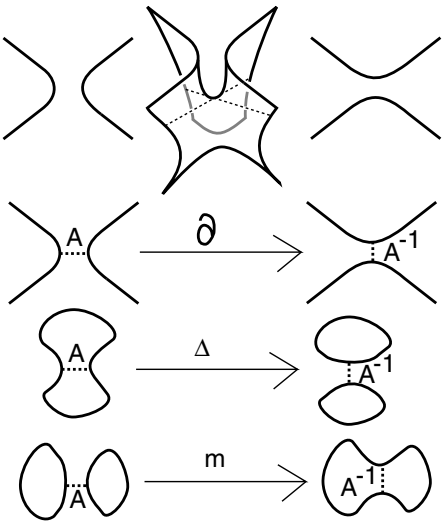


FIGURE 2. **SaddlePoints and State Smoothings**

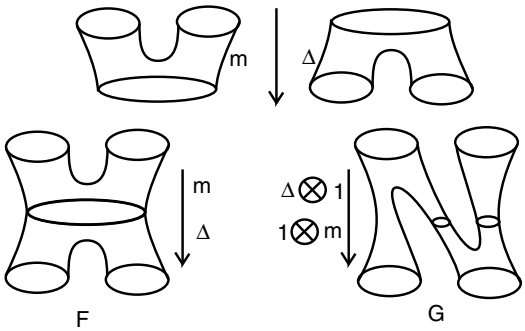


FIGURE 3. **Surface Cobordisms**

just as in a de Rahm complex. The Grassmann algebra automatically computes the correct signs in the chain complex, and this boundary formula gives the original boundary formula when we take coefficients modulo two. Note, that in this formalism, partial differentials ∂_i of enhanced states with a B-smoothing at the site i are zero due to the fact that $dx_i \wedge dx_i = 0$ in the Grassmann algebra. There is more to discuss about the use of Grassmann algebra in this context. For example, this approach clarifies parts of the construction in [**19**].

It of interest to examine this analogy between the Khovanov (co)homology and de Rahm cohomology. In that analogy the enhanced states correspond to the differentiable functions on a manifold. The Khovanov complex $C^k(K)$ is generated by elements of the form $s\, dx_{i_1} \wedge \cdots \wedge dx_{i_k}$ where the enhanced state s has B-smoothings at exactly the sites $i_1, \cdots, i_k$. If we were to follow the analogy with de Rahm cohomology literally, we would define a new complex $DR(K)$ where $DR^k(K)$ is generated by elements $s\, dx_{i_1} \wedge \cdots \wedge dx_{i_k}$ where s is *any* enhanced state of the link K. The partial boundaries are defined in the same

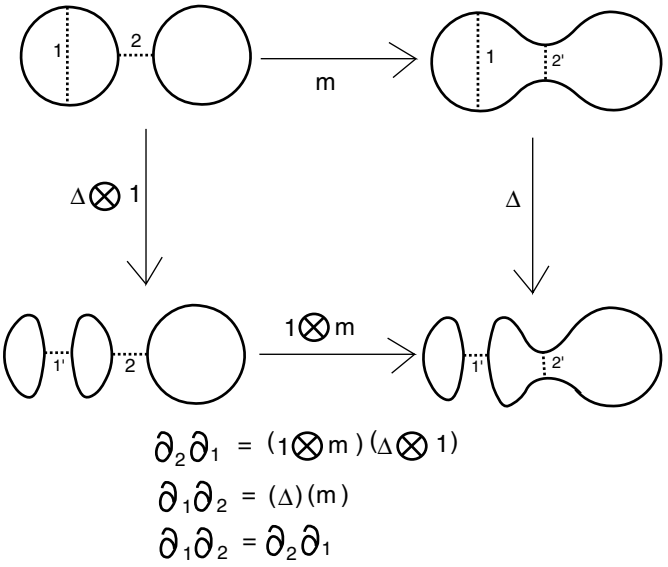


FIGURE 4. **Local Boundaries Commute**

way as before and the global boundary formula is just as we have written it above. This gives a *new* chain complex associated with the link K. Whether its homology contains new topological information about the link K will be the subject of a subsequent paper.

In the case of de Rhanm cohomology, we can also look for compatible unitary transformations. Let M be a differentiable manifold and $\mathcal{C}(M)$ denote the DeRham complex of M over the complex numbers. Then for a differential form of the type $f(x)\omega$ in local coordinates $x_1, \cdots, x_n$ and ω a wedge product of a subset of $dx_1 \cdots dx_n$, we have

$$d(f\omega) = \sum_{i=1}^{n} (\partial f/\partial x_i) dx_i \wedge \omega.$$

Here d is the differential for the DeRham complex. Then $\mathcal{C}(M)$ has as basis the set of $|f(x)\omega\rangle$ where $\omega = dx_{i_1} \wedge \cdots \wedge dx_{i_k}$ with $i_1 < \cdots < i_k$. We could achieve $Ud + dU = 0$ if U is a very simple unitary operator (e.g. multiplication by phases that do not depend on the coordinates x_i) but in general it will be an interesting problem to determine all unitary operators U with this property.

A further remark on de Rham cohomology. There is another deep relation with the de Rham complex: In [**22**] it was observed that Khovanov homology is related to Hochschild homology and Hochschild homology is thought to be an algebraic version of de Rham chain complex (cyclic cohomology corresponds to de Rham cohomology), compare [**24**].

7. The Simplicial Structure of Khovanov Homology

Let $\mathcal{S}$ denote the set of (standard) bracket states for a link diagram K. Another way to describe the Khovanov complex is to associate to each state loop λ a module V isomorphic to the algebra $k[x]/(x^2)$ with coproduct as we have described in the previous section. The generators 1 and x of this algebra can then be regarded as the two possible enhancements

of the loop λ. In the same vein we associate to a state S the tensor product of copies of V, one copy for each loop in the state. The local boundaries are defined exactly as before, and the Khovanov complex is the direct sum of the modules associated with the states of the link diagram. We will use this point of view in the present section, and we shall describe Khovanov homology in terms of a very natural " n-cube category" and an associated simplicial object. The purpose of this section is to move towards, albeit in an abstract manner, a description of Khovanov homology as the homology of a topological space. We do not accomplish this aim, but the constrctions given herein may move toward that goal. An intermediate possibility would be to replace the Khovanov homology by an abstract space or simplicial object whose homotopy type was in invariant of the knot or link. There is a second motivation for our construction, in that it is interesting to have a second formulation of the genesis of the Hilbert space that we have used in this paper. We have identified this Hilbert space as the chain complex for Khovanov homology. Now we shall see that this chain complex derives from a natural simplicial structure that can be seen as a background lattice for the quantum algorithms of this paper.

Let $\mathcal{D}^n = \{A, B\}^n$ be the n-cube category whose objects are the n-sequences from the set $\{A, B\}$ and whose morphisms are arrows from sequences with greater numbers of A's to sequences with fewer numbers of A's. Thus $\mathcal{D}^n$ is equivalent to the poset category of subsets of $\{1, 2, \cdots n\}$. Let $\mathcal{M}$ be a pointed category with finite sums, and let $\mathcal{F} : \mathcal{D}^n \longrightarrow \mathcal{M}$ be a functor. In our case $\mathcal{M}$ is a category of modules (as described above) and $\mathcal{F}$ carries n-sequences to certain tensor powers corresponding to the standard bracket states of a knot or link K. We map sequences to states by choosing to label the crossings of the diagram K from the set $\{1, 2, \cdots n\}$, and letting the functor take abstract A's and B's in the cube category to smoothings at those crossings of type A or type B. Thus each sequence in the cube category is associated with a unique state of K when K has n crossings. Nevertheless, we shall describe the construction more generally.

For the functor $\mathcal{F}$ we first construct a semisimplicial object $\mathcal{C}(F)$ over $\mathcal{M}$, where a semisimplicial object is a simplicial object without degeneracies. This means that it has partial boundaries analogous to the partial boundaries that we have discussed before but none of the degeneracy maps that are common to simplicial theory (see [**25**] Chapter 1). For $k \geq 0$ we set

$$\mathcal{C}(F)_k = \oplus_{v \in \mathcal{D}^n_k} \mathcal{F}(v)$$

where $\mathcal{D}^n_k$ denotes those sequences in the cube category with k A's. Note that we are indexing dually to the upper indexing in the Khovanov homology sections of this paper where we counted the number of B's in the states.

We introduce face operators (partial boundaries in our previous terminology)

$$d_i : \mathcal{C}(F)_k \longrightarrow \mathcal{C}(F)_{k-1}$$

for $0 \leq i \leq k$ with $k \geq 1$ as follows: d_i is trivial for $i = 0$ and otherwise d_i acts on $\mathcal{F}(v)$ by the map $\mathcal{F}(v) \longrightarrow \mathcal{F}(v')$ where v' is the sequence resulting from replacing the i-th A by B. The operators d_i satisfy the usual face relations of simplicial theory:

$$d_i d_j = d_{j-1} d_i$$

for $i < j$.

We now expand $\mathcal{C}(F)$ to a simplicial object $\mathcal{S}(F)$ over $\mathcal{M}$ by applying freely degeneracies to the $\mathcal{F}(v)$'s. Thus

$$\mathcal{S}(F)_m = \oplus_{v \in \mathcal{D}^n_k, k+t=m} \; s_{i_1} \cdots s_{i_t} \mathcal{F}(v)$$

where $m > i_1 > \cdots > i_t \geq 0$ and these degeneracy operators are applied freely modulo the usual (axiomatic) relations among themselves and with the face operators. Then $\mathcal{S}(F)$ has degeneracies via formal application of degeneracy operators to these forms, and has face operators extending those of $\mathcal{C}(\mathcal{F})$. It is at this point we should remark that in our knot theoretic construction there is only at this point an opportunity for formal extension of degeneracy operators above the number of crossings in the given knot or link diagram since to make specific degeneracies would involve the creation of new diagrammatic sites. There may be a natural construction of this sort and if there is, such a construction could lead to a significant homotopy theory for Khovanov homology.

When the functor $\mathcal{F} : \mathcal{D}^n \longrightarrow \mathcal{M}$ goes to an abelian category $\mathcal{M}$, as in our knot theoretic case, we can recover the homology groups via

$$H_\star N\mathcal{S}(\mathcal{F}) \cong H_\star \mathcal{C}(\mathcal{F})$$

where $N\mathcal{S}(\mathcal{F}$ is the normalized chain complex of $\mathcal{S}(\mathcal{F})$. This completes the abstract simplicial description of this homology.

This simplicial description of Khovanov homology lets us make a larger conceptualization of the possible relationship of homology and a Hilbert space with its quantum dynamics and measurement. The natural Hilbert space to take in the context of this section is the space whose basis is the set of A, B sequences that form the objects of the n-cube category $\mathcal{D}^n$. We then see that a functor $\mathcal{F} : \mathcal{D}^n \longrightarrow \mathcal{M}$ to a module category $\mathcal{M}$ provides the extra structure of Hilbert space on $\mathcal{C}(\mathcal{F})$ that supports the homology $H_\star \mathcal{C}(\mathcal{F})$. In the case of Khovanov homology, this extra structure amounts to the enhancements of the standard bracket states. The standard bracket states are in 1-1 correspondence with the sequences in $\mathcal{D}^n$ and so we have a very concrete description of this functorial relationship. But more generally, the categorical picture shows how a basic Hilbert space is boosted to acquire new elements and extra structure that allow it to support non-trivial homology and unitary transformations that respect that homology. There is clearly much work to be done in exploring this relationship of quantum information and algebraic topology.

8. Appendix - The Hadamard Test

In order to make a quantum computation of the trace of a unitary matrix U, one can use the *Hadamard test* to obtain the diagonal matrix elements $\langle \psi | U | \psi \rangle$ of U. The trace is then the sum of these matrix elements as $|\psi\rangle$ runs over an orthonormal basis for the vector space. In the application to the algorithm described here for the Jones polynomial it is only necessary to compute one number of the form $\langle \psi | U | \psi \rangle$. The Hadamard test proceeds as follows.

We first obtain

$$\frac{1}{2} + \frac{1}{2} Re \langle \psi | U | \psi \rangle$$

as an expectation by applying the Hadamard gate H

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

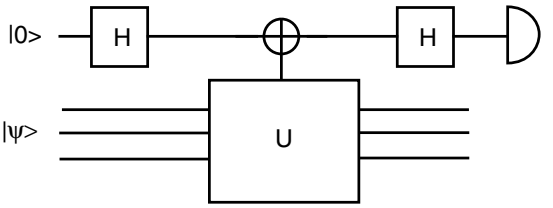


FIGURE 5. **Hadamard Test**

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

to the first qubit of

$$C_U \circ (H \otimes 1)|0\rangle|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle + |1\rangle \otimes U|\psi\rangle.$$

Here C_U denotes controlled U, acting as U when the control bit is $|1\rangle$ and the identity mapping when the control bit is $|0\rangle$. We measure the expectation for the first qubit $|0\rangle$ of the resulting state

$$(H \otimes 1) \circ C_U \circ (H \otimes 1)|0\rangle|\psi\rangle =$$

$$\frac{1}{2}(H|0\rangle \otimes |\psi\rangle + H|1\rangle \otimes U|\psi\rangle) = \frac{1}{2}((|0\rangle + |1\rangle) \otimes |\psi\rangle + (|0\rangle - |1\rangle) \otimes U|\psi\rangle)$$

$$= \frac{1}{2}(|0\rangle \otimes (|\psi\rangle + U|\psi\rangle) + |1\rangle \otimes (|\psi\rangle - U|\psi\rangle)).$$

This expectation is

$$\frac{1}{4}(\langle\psi| + \langle\psi|U^\dagger)(|\psi\rangle + U|\psi\rangle) = \frac{1}{2} + \frac{1}{2}Re\langle\psi|U|\psi\rangle.$$

In Figure 5, we illustrate this computation with a diagram that indicates the structure of the test with parallel lines corresponding to tensor products of the single qubit space (with three lines chosen for illustration as the size of U). The extra tensor factor is indicated on the top line with the Hadamard matrix H indicated by a box and the control of U indicated by a circle with a vertical control line extending down to the U-box. The half -circle on the top line on the right stands for the measurement of that line that is used for the computation. Thus Figure 5 represents a circuit diagram for the quantum computation of $\frac{1}{2} + \frac{1}{2}Re\langle\psi|U|\psi\rangle$ and hence the quantum computation of $\frac{1}{2} + \frac{1}{2}Re\langle K\rangle$ when U is taken to be the unitary tranformation corresponding to the bracket polynomial, as discussed in previous sections of this paper.

The imaginary part is obtained by applying the same procedure to

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |\psi\rangle - i|1\rangle \otimes U|\psi\rangle)$$

This is the method used in **[1, 15, 16]**, and the reader may wish to contemplate its efficiency in the context of this simple model. Note that the Hadamard test enables this quantum computation to estimate the trace of any unitary matrix U by repeated trials that estimate individual matrix entries $\langle\psi|U|\psi\rangle$.

References

[1] D. Aharonov, V. Jones, Z. Landau, A polynomial quantum algorithm for approximating the Jones polynomial, quant-ph/0511096.

[2] Bar–Natan, D. (2002), On Khovanov's categorification of the Jones polynomial, *Algebraic and Geometric Topology*, **2**(16), pp. 337–370.

[3] Bar-Natan, D. (2005), Khovanov's homology for tangles and cobordisms, *Geometry and Topology*, **9-33**, pp. 1465-1499. arXiv:mat.GT/0410495

[4] R.J. Baxter, Exactly Solved Models in Statistical Mechanics, Acad. Press (1982).

[5] R. Dijkgraaf, D. Orland and S. Reffert, Dimer models, free fermions and super quantum mechanics, arXiv:0705.1645.

[6] S. Gukov, Surface operators and knot homologies, ArXiv:0706.2369.

[7] L.Helme-Guizon, J.H.Przytycki, Y.Rong, Torsion in Graph Homology, *Fundamenta Mathematicae*, 190; June 2006, 139–177.

[8] V.F.R. Jones, A polynomial invariant for links via von Neumann algebras, Bull. Amer. Math. Soc. **129** (1985), 103–112.

[9] V.F.R.Jones. Hecke algebra representations of braid groups and link polynomials, Ann. of Math. 126 (1987), pp. 335-338.

[10] V.F.R.Jones, On knot invariants related to some statistical mechanics models, Pacific J. Math., vol. 137, no. 2 (1989), pp. 311-334.

[11] L.H. Kauffman, State models and the Jones polynomial, Topology **26** (1987), 395–407.

[12] L.H. Kauffman, Statistical mechanics and the Jones polynomial, AMS Contemp. Math. Series **78** (1989), 263–297.

[13] L.H. Kauffman, *Knots and Physics*, World Scientific Publishers (1991), Second Edition (1993), Third Edition (2002).

[14] L.H. Kauffman, Topological Quantum Information, Khovanov Homology and the Jones Polynomial, arXiv:1001.0354

[15] L.H. Kauffman, Quantum computing and the Jones polynomial, in *Quantum Computation and Information*, S. Lomonaco, Jr. (ed.), AMS CONM/305, 2002, pp. 101–137. math.QA/0105255

[16] L. H. Kauffman and S. Lomonaco Jr., A Three-stranded quantum algorithm for the Jones polynonmial, in "Quantum Information and Quantum Computation V", Proceedings of Spie, April 2007, edited by E.J. Donkor, A.R. Pirich and H.E. Brandt, pp. 65730T1-17, Intl Soc. Opt. Eng.

[17] S. J. Lomonaco Jr. and L. H. Kauffman, Quantum Knots and Mosaics, Journal of Quantum Information Processing, Vol. 7, Nos. 2-3, (2008), pp. 85 - 115. arxiv.org/abs/0805.0339

[18] H.A. Dye, L.H. Kauffman, V.O. Manturov, On two categorifications of the arrow polynomial for virtual knots, arXiv:0906.3408.

[19] V.O. Manturov, Khovanov homology for virtual links with arbitrary coefficients, math.GT/0601152.

[20] Khovanov, M. (1997), A categorification of the Jones polynomial, *Duke Math. J*,**101** (3), pp.359-426.

[21] Lee, T. D., Yang, C. N. (1952), Statistical theory of equations of state and phase transitions II., lattice gas and Ising model, *Physical Review Letters*, **87**, 410-419.

[22] J. H. Przytycki, When the theories meet: Khovanov homology as Hochschild homology of links, arXiv:math.GT/0509334

[23] S. Lang, Algebra, Springer-Verlag, New York, Inc. (2002).

[24] J-L. Loday, Cyclic Homology, Grund. Math. Wissen. Band 301, Springer-Verlag, Berlin, 1992 (second edition, 1998).

[25] J. P. May, "Simplicial Objects in Algebraic Topology", University of Chicago Press (1967).

[26] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press (2000).

[27] E.F. Jasso-Hernandez and Y. Rong, A categorification of the Tutte polynomial, *Alg. Geom. Topology* **6** 2006, 2031-2049.

[28] Raimund Marx, Amr Fahmy, Louis Kauffman, Samuel Lomonaco, Andreas Spörl, Nikolas Pomplun, John Myers, Steffen J. Glaser, NMR Quantum Calculations of the Jones Polynomial, arXiv:0909.1080.

[29] M. Stosic, Categorification of the dichromatic polynomial for graphs, arXiv:Math/0504239v2, *JKTR*, Vol. 17, No. 1, (2008), pp. 31-45.

[30] O. Viro (2004), Khovanov homology, its definitions and ramifications, *Fund. Math.*, **184** (2004), pp. 317-342.

[31] E. Witten. Quantum Field Theory and the Jones Polynomial. Comm. in Math. Phys. Vol. 121 (1989), 351-399.

DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTER SCIENCE (M/C 249), 851 SOUTH MORGAN STREET, UNIVERSITY OF ILLINOIS AT CHICAGO, CHICAGO, ILLINOIS 60607-7045
E-mail address: kauffman@uic.edu

Contemporary Mathematics
Volume **536**, 2011

Oriented Quantum Algebras and Coalgebras, Invariants of Oriented 1–1 Tangles, Knots and Links

Louis Kauffman and David E. Radford

Abstract. This paper is the third in a series on oriented quantum algebras, structures related to them, and regular isotopy invariants associated with them. There is always a regular isotopy invariant of oriented 1–1 tangles associated to an oriented quantum algebra. Regular isotopy invariants of oriented knots and links can be constructed from oriented quantum algebras with a bit more structure. These are the twist oriented quantum algebras and they account for a very large number of the known regular isotopy invariants of oriented knots and links.

In this paper we study oriented quantum coalgebras which are structures closely related to oriented quantum algebras. We study the relationship between oriented quantum coalgebras and oriented quantum algebras and the relationship between oriented quantum coalgebras and quantum coalgebras. We show that there are regular isotopy invariants of oriented 1–1 tangles and of oriented knots and links associated to oriented and twist oriented quantum coalgebras respectively. There are many parallels between the theory of oriented quantum coalgebras and the theory of quantum coalgebras; the latter are introduced and studied in [**11**].

In the first paper [**9**] of this series the notion of oriented quantum algebra is introduced in the context of a very natural diagrammatic formalism. In the second [**8**] basic properties of oriented quantum algebras are described. Several examples of oriented quantum algebras are given, one of which is a paramaterized family which accounts for the Jones and HOMFLY polynomials.

1. Introduction

There is an extensive literature on invariants of tangles, knots, or links derived from Hopf algebras. We refer the reader to two basic ones here [**17, 18**].

This paper is organized as follows. In Section 2 we review most of the coalgebra prerequisites for this paper. Not much is required. The theory of coalgebras needed for this paper is more than adequately covered in any of [**12, 13, 19**]. In Section 3 we review the notions of quantum algebra, quantum coalgebra and their oriented counterparts. We also recall examples of oriented quantum algebras described in

1991 *Mathematics Subject Classification.* 16T15, 16W99.

Key words and phrases. oriented quantum algebras and coalgebras, invariants of knots and links.

Research supported in part by NSF Grant DMS 920-5227.

Research supported in part by NSF Grant DMS 980 2178.

[**9, 10**]. We explore duality relationships between oriented algebra and coalgebra structures.

Section 4 is devoted to the relationship between oriented quantum algebras and quantum algebras. We have shown that a quantum algebra has an oriented quantum algebra structure. Here we show how to associate a quantum algebra to an oriented quantum algebra in a very natural way. In Section 5 we prove some general results on oriented quantum coalgebras. Section 6 is the coalgebra version of Section 4.

In Section 7 we define a function from the set of oriented 1–1 tangle diagrams with respect to a vertical to the dual algebra of an oriented quantum coalgebra and prove that this function determines a regular isotopy invariant of oriented 1–1 tangles. In Section 8 we show that the invariant of Section 7 is no better than the writhe when the oriented quantum coalgebra is cocommutative. One would expect this to be the case since the invariant of oriented 1–1 diagrams constructed from a commutative oriented quantum algebra has the same property.

In Section 9 the construction of the invariant of oriented 1–1 tangles described in Section 7 is used to give an invariant of oriented knots and links when the oriented quantum coalgebra is a twist oriented quantum coalgebra. The invariant for knots and links is a scalar.

This paper and some of its results were described in the survey paper [**16**]. Throughout k is a field and $k^\star$ will denote the set of non-zero elements of k.

2. Preliminaries

For vector spaces U and V over k we will denote the tensor product $U\otimes_k V$ by $U\otimes V$, the identity map of V by 1_V and the linear dual $\mathrm{Hom}_k(V,k)$ of V by V^*. If T is a linear endomorphism of V then an element $v\in V$ is *T-invariant* if $T(v)=v$. If A is an algebra over k we shall let 1_A also denote the unit of k. Then meaning 1_V should always be clear from context.

We will usually denote a coalgebra (C,Δ,ϵ) over k by C and we will follow the convention of writing the coproduct $\Delta(c)$ symbolically as $\Delta(c)=c_{(1)}\otimes c_{(2)}$ for all $c\in C$. This way of writing $\Delta(c)$ is a variation of the Heyneman–Sweedler notation. The *opposite coalgebra*, which we denote by C^{cop}, is $(C,\Delta^{cop},\epsilon)$, where $\Delta^{cop}(c)=c_{(2)}\otimes c_{(1)}$ for all $c\in C$. An element $c\in C$ is said to be *cocommutative* if $\Delta(c)=c_{(2)}\otimes c_{(1)}=\Delta^{cop}(c)$. The coalgebra C is said to be a *cocommutative coalgebra* if all of its elements are cocommutative, or equivalently if $C=C^{cop}$.

Set $\Delta^{(1)}=\Delta$ and define $\Delta^{(n)}: C\longrightarrow C\otimes\cdots\otimes C$ ($n+1$ summands) for $n>1$ inductively by $\Delta^{(n)}=(\Delta\otimes 1_C\otimes\cdots\otimes 1_C)\circ\Delta^{(n-1)}$. We generalize our notation for the coproduct and write $\Delta^{(n-1)}(c)=c_{(1)}\otimes c_{(2)}\otimes\cdots\otimes c_{(n)}$ for all $c\in C$.

A coalgebra which the reader will encounter several times in this paper is the *comatrix coalgebra* $\mathrm{C}_n(k)$ which is defined for all $n\geq 1$. As a k-vector space $\mathrm{C}_n(k)$ has basis $\{e^\imath_\jmath\}_{1\leq\imath,\jmath\leq n}$. The coproduct and the counit for $\mathrm{C}_n(k)$ are determined by

$$\Delta(e^\imath_\jmath)=\sum_{\ell=1}^{n} e^\imath_\ell\otimes e^\ell_\jmath \quad\text{and}\quad \epsilon(e^\imath_\jmath)=\delta^\imath_\jmath$$

respectively for all $1\leq\imath,\jmath\leq n$.

We usually denote an algebra (A,m,η) over k by A. The *opposite algebra* is the k-algebra (A,m^{op},η) whose product is defined by $m^{op}(a\otimes b)=m(b\otimes a)=ba$ for all $a,b\in A$. We denote the opposite algebra by A^{op}. For $n\geq 1$ let $\mathrm{M}_n(k)$ the

algebra of all $n\times n$ matrices with entries in k and let $\{E^\imath_\jmath\}_{1\le\imath,\jmath\le n}$ be the standard basis for $\mathrm{M}_n(k)$. In our notation $E^\imath_\jmath E^\ell_m = \delta^\ell_\jmath E^\imath_m$ for all $1 \le \imath, \jmath, \ell, m \le n$.

Let C be a coalgebra over k. Then C^* is an algebra over k, called the *dual algebra*, or *algebra dual to* C, whose product is determined by

$$c^*d^*(c) = c^*(c_{(1)})d^*(c_{(2)})$$

for all $c^*, d^* \in C^*$ and $c \in C$ and whose unit is ϵ. Note that C is a C^*-bimodule under the left and right actions

$$c^* \rightharpoonup c = c_{(1)}c^*(c_{(2)}) \quad \text{and} \quad c \leftharpoonup c^* = c^*(c_{(1)})c_{(2)}$$

for all $c^* \in C^*$ and $c \in C$.

Now suppose that A is an algebra over k. Then the subspace A^o of A^* consisting of all functionals which vanish on a cofinite ideal of A is a coalgebra over k. For $a^o \in A^o$ the coproduct $\Delta(a^o) = \sum_{\imath=1}^r a^o_\imath \otimes b^o_\imath$ is determined by

$$a^o(ab) = \sum_{\imath=1}^r a^o_\imath(a)b^o_\imath(b)$$

for all $a, b \in A$ and the counit is given by $\epsilon(a^o) = a^o(1)$. If $f : A \longrightarrow B$ is an algebra map then the restriction f^o of the transpose map $f^* : B^* \longrightarrow A^*$ determines a coalgebra map $f^o : B^o \longrightarrow A^o$. Note that $A^o = A^*$ when A is finite-dimensional. Observe that $\mathrm{C}_n(k) \simeq \mathrm{M}_n(k)^*$ as coalgebras and that $\{e^\imath_\jmath\}_{1\le\imath,\jmath\le n}$ can be identified with the basis for $\mathrm{C}_n(k)$ dual to the standard basis $\{E^\imath_\jmath\}_{1\le\imath,\jmath\le n}$ for $\mathrm{M}_n(k)$.

Let V be a vector space over k and suppose that $b : V\times V \longrightarrow k$ is a bilinear form. We define $b_{(\ell)}, b_{(r)} : V \longrightarrow V^*$ by $b_{(\ell)}(u)(v) = b(u, v) = b_{(r)}(v)(u)$ for all $u, v \in V$. For $\rho \in V\otimes V$ we define a bilinear form $b_\rho : V^*\otimes V^* \longrightarrow k$ by $b_\rho(u^*, v^*) = (u^*\otimes v^*)(\rho)$ for all $u^*, v^* \in V^*$.

Now suppose that C, D are coalgebras over k and let $b, b' : C\times D \longrightarrow k$ be bilinear forms. Then b' is an *inverse for* b if

$$b'(c_{(1)}, d_{(1)})b(c_{(2)}, d_{(2)}) = \epsilon(c)\epsilon(d) = b(c_{(1)}, d_{(1)})b'(c_{(2)}, d_{(2)})$$

for all $c \in C$ and $d \in D$. The bilinear form b has at most one inverse which we denote b^{-1} when it exists.

3. Oriented Quantum Algebras and Coalgebras, Definitions and Examples

In this section we recall the definition of quantum algebra, oriented quantum algebra, quantum coalgebra and oriented quantum coalgebra and list some examples of these structures which are found in [**9**] and [**10**]. We consider duality relations between these algebra and coalgebra structures.

An important component of the definition of quantum algebra or oriented quantum algebra is a solution to a the quantum Yang–Baxter equation. Let A be an algebra over the field k, $\rho \in A\otimes A$ and write $\rho = \sum_{\imath=1}^r a_\imath\otimes b_\imath$. For $1 \le \imath < \jmath \le 3$ let $\rho_{\imath\,\jmath} \in A\otimes A\otimes A$ be defined by

$$\rho_{1\,2} = \sum_{\imath=1}^r a_\imath\otimes b_\imath\otimes 1, \quad \rho_{1\,3} = \sum_{\imath=1}^r a_\imath\otimes 1\otimes b_\imath \quad \text{and} \quad \rho_{2\,3} = \sum_{\imath=1}^r 1\otimes a_\imath\otimes b_\imath.$$

The quantum Yang–Baxter equation for ρ is $\rho_{1\,2}\rho_{1\,3}\rho_{2\,3} = \rho_{2\,3}\rho_{1\,3}\rho_{1\,2}$.

The notion of quantum algebra is defined in [**4**]. A *quantum algebra* over the field k is a triple (A, ρ, s), where A is an algebra over k, $\rho \in A \otimes A$ is invertible and $s : A \longrightarrow A^{op}$ is an algebra isomorphism, such that

(QA.1) $\rho^{-1} = (s \otimes 1_A)(\rho)$,

(QA.2) $\rho = (s \otimes s)(\rho)$ and

(QA.3) $\rho_{1\,2}\rho_{1\,3}\rho_{2\,3} = \rho_{2\,3}\rho_{1\,3}\rho_{1\,2}$.

Suppose that (A', ρ', s') is a quantum algebra over k also. A *morphism of quantum algebras* $f : (A, \rho, s) \longrightarrow (A', \rho', s')$ is an algebra map $f : A \longrightarrow A'$ which satisfies $\rho' = (f \otimes f)(\rho)$ and $s' \circ f = f \circ s$. Quantum algebras together with their morphisms under composition form a monoidal category. The reader is referred to [**11**, Section 3] at this point.

Our first example of a quantum algebra accounts for the Jones polynomial when $k = \mathbb{C}$ is the field of complex numbers. See [**4**, page 580] and also [**10**, Section 3].

EXAMPLE 1. *Let $q \in k^\star$. Then $(\mathrm{M}_2(k), \rho, s)$ is a quantum algebra over the field k, where*

$$\rho = q^{-1}(E_1^1 \otimes E_1^1 + E_2^2 \otimes E_2^2) + q(E_1^1 \otimes E_2^2 + E_2^2 \otimes E_1^1) + (q^{-1} - q^3)E_2^1 \otimes E_1^2$$

and $s(x) = MxM^{-1}$ for all $x \in \mathrm{M}_2(k)$, where $M = \begin{pmatrix} 0 & q \\ -q^{-1} & 0 \end{pmatrix}$.

Finite-dimensional quasitriangular Hopf algebras account for a large class of quantum algebras.

EXAMPLE 2. *Let (A, ρ) be a quasitriangular Hopf algebra with antipode s over the field k. Then (A, ρ, s) is a quantum algebra over k.*

The notion of oriented quantum algebra is introduced in [**9**, Section 1]. An *oriented quantum algebra* over the field k is a quadruple $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$, where A is an algebra over k, $\rho \in A \otimes A$ is invertible and $t_{\mathsf{d}}, t_{\mathsf{u}}$ are commuting algebra automorphisms of A, such that

(qa.1) $(t_{\mathsf{d}} \otimes 1_A)(\rho^{-1})$ and $(1_A \otimes t_{\mathsf{u}})(\rho)$ are inverses in $A \otimes A^{op}$,

(qa.2) $\rho = (t_{\mathsf{d}} \otimes t_{\mathsf{d}})(\rho) = (t_{\mathsf{u}} \otimes t_{\mathsf{u}})(\rho)$ and

(qa.3) $\rho_{1\,2}\rho_{1\,3}\rho_{2\,3} = \rho_{2\,3}\rho_{1\,3}\rho_{1\,2}$.

An oriented quantum algebra $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is *standard* if $t_{\mathsf{d}} = 1_A$ and is *balanced* if $t_{\mathsf{d}} = t_{\mathsf{u}}$. In the balanced case we write (A, ρ, t) for (A, ρ, t, t).

Suppose that $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ and $(A, \rho', t'_{\mathsf{d}}, t'_{\mathsf{u}})$ are oriented quantum algebras over k. A *morphism of oriented quantum algebras* $f : (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}}) \longrightarrow (A', \rho', t'_{\mathsf{d}}, t'_{\mathsf{u}})$ is an algebra map $f : A \longrightarrow A'$ which satisfies $\rho' = (f \otimes f)(\rho)$, $t'_{\mathsf{d}} \circ f = f \circ t_{\mathsf{d}}$ and $t'_{\mathsf{u}} \circ f = f \circ t_{\mathsf{u}}$. Oriented quantum algebras together with their morphisms under composition form a monoidal category.

Theorem 1 of [**9**] accounts for an extensive family of examples of balanced oriented quantum algebras.

EXAMPLE 3. *Let $n \geq 2$ and $x, \hbar \in k^\star$. Then $(\mathrm{M}_n(k), \rho, t)$ is a balanced oriented quantum algebra over k where $\rho = \sum_{\imath,\jmath,\ell,m=1}^{n} \rho_{\jmath\,m}^{\imath\,\ell} E_\jmath^\imath \otimes E_m^\ell$ satisfies*

a) $\rho_{\jmath\,m}^{\imath\,\ell} = 0$ *unless* $\{\imath, \ell\} = \{\jmath, m\}$,
b) $\rho_{\imath\,\jmath}^{\imath\,\jmath} \neq 0$ *for all* $1 \leq \imath, \jmath \leq n$,
c) $\rho_{\jmath\,\imath}^{\imath\,\jmath} = x = \rho_{\imath\,\imath}^{\imath\,\imath} - \hbar/\rho_{\imath\,\imath}^{\imath\,\imath}$ *and* $\rho_{\imath\,\jmath}^{\jmath\,\imath} = 0$ *for all* $1 \leq \imath < \jmath \leq n$,

d) $\rho^{\imath\jmath}_{\imath\jmath}\rho^{\jmath\imath}_{\jmath\imath} = bc$ *for all* $1 \le \imath < \jmath \le n$,

e) *for all* $1 \le \imath, \jmath \le n$ *either* $\rho^{\imath\imath}_{\imath\imath} = \rho^{\jmath\jmath}_{\jmath\jmath}$ *or* $\rho^{\imath\imath}_{\imath\imath}\rho^{\jmath\jmath}_{\jmath\jmath} = -bc$

and $t(E^{\imath}_{\jmath}) = (\omega_{\imath}/\omega_{\jmath})E^{\imath}_{\jmath}$ *for all* $1 \le \imath, \jmath \le n$, *where* $\omega_1, \dots, \omega_n \in k^{\star}$ *satisfy*

$$\omega_{\imath}^2 = \left(\frac{\rho^{1\,1}_{1\,1}\rho^{\imath\imath}_{\imath\imath}}{bc}\right)\left(\prod_{1<\jmath<\imath}\frac{(\rho^{\jmath\jmath}_{\jmath\jmath})^2}{bc}\right)\omega_1^2$$

for all $1 < \imath \le n$.

Let $k = \mathbb{C}$ be the field of complex numbers and suppose that $q \in \mathbb{C}^*$ is transcendental over the subfield of rational numbers. When $bc = q^2$, $x = q^{-1} - q^3$, $\rho^{\imath\imath}_{\imath\imath} = q^{-1}$ for all $1 \le \imath \le n$ and $\rho^{\imath\jmath}_{\imath\jmath} = q^2$ whenever $1 \le \imath, \jmath \le n$ are distinct, then Example 3 accounts for the HOMFLY polynomial.

A quantum algebra always has an oriented quantum algebra structure by virtue of [**8**, Propositions 1 and 2].

EXAMPLE 4. *If* (A, ρ, s) *is a quantum algebra over the field* k *then* $(A, \rho, s^{-2}, 1_A)$ *and* $(A, \rho, 1_A, s^{-2})$ *are oriented quantum algebras over* k.

A quantum algebra (A, ρ, s) over k may have no oriented quantum algebra structures of the type $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ except those mentioned in the preceding example; see Example 4 of [**8**]. A balanced oriented quantum algebra (A, ρ, t) over k may not have a quantum algebra structure of the type (A, ρ, s); see Example 3 of [**8**].

Balanced oriented quantum algebras arise in very natural ways.

EXAMPLE 5. *Let* (A, ρ) *be a finite-dimensional quasitriangular Hopf algebra over the field* k *and suppose that* t *is a Hopf algebra automorphism of* A *which satisfies* $\rho = (t\otimes t)(\rho)$ *and* $t^2 = s^{-2}$. *Then* (A, ρ, t) *is a balanced oriented quantum algebra.*

Very important examples of a finite-dimensional quasitriangular Hopf algebras over k are the quantum doubles $(D(A), \boldsymbol{\rho})$ of finite-dimensional Hopf algebras A with antipode s over k. We write $D(A) = A^*\otimes A$ as a vector space.

EXAMPLE 6. *Let* A *be a finite-dimensional Hopf algebra over* k *and suppose that* t *is a Hopf algebra automorphism of* A *which satisfies* $t^2 = s^{-2}$. *Then* $(D(A), \boldsymbol{\rho}, T)$ *is a balanced oriented quantum algebra over* k, *where* $T = (t^{-1})^*\otimes t$.

For details concerning these two examples see [**9**, Corollary 2] and the discussion preceding it.

We now turn to quantum coalgebras and oriented quantum coalgebras. The notion of quantum coalgebra was introduced in [**11**, Section 4]. Strict quantum coalgebras form an important class of quantum coalgebras.

A *strict quantum coalgebra over* k is a triple (C, b, S), where C is a coalgebra over k, $b : C\times C \longrightarrow k$ is an invertible bilinear form and $S : C \longrightarrow C^{cop}$ is a coalgebra isomorphism, such that

(QC.1) $b^{-1}(c, d) = b(S(c), d)$,

(QC.2) $b(c, d) = b(S(c), S(d))$ and

(QC.3) $b(c_{(1)}, d_{(1)})b(c_{(2)}, e_{(1)})b(d_{(2)}, e_{(2)}) = b(c_{(2)}, d_{(2)})b(c_{(1)}, e_{(2)})b(d_{(1)}, e_{(1)})$

for all $c, d, e \in C$. A *quantum coalgebra over* k is a triple (C, b, S), where C is a coalgebra over k, $b : C\times C \longrightarrow k$ is an invertible bilinear form, $S : C \longrightarrow C^{cop}$ is a coalgebra isomorphism of C with respect to b, such that (QC.1)–(QC.3) hold. That

S is a coalgebra isomorphism with respect to b means S is a linear isomorphism which satisfies $\epsilon \circ S = \epsilon$,

$$b(S(c_{(1)}), d)b(S(c_{(2)}), e) = b(S(c)_{(2)}, d)b(S(c)_{(1)}, e) \text{ and}$$
$$b(d, S(c_{(1)}))b(e, S(c_{(2)})) = b(d, S(c)_{(2)})b(e, S(c)_{(1)})$$

for all $c, d, e \in C$.

A *morphism of quantum coalgebras* $f : (C, b, S) \longrightarrow (C', b', S')$ is a coalgebra map $f : C \longrightarrow C'$ which satisfies $b(c, d) = b'(f(c), f(d))$ for all $c, d \in C$ and $S' \circ f = f \circ S$. Quantum coalgebras over k together with their morphisms under composition form a monoidal category; the strict quantum coalgebras over k form a subcategory of this category.

The notions of quantum algebra and strict quantum coalgebra are dual as was remarked in [**11**, Section 4.1]. More formally,

PROPOSITION 1. *Let A be a finite-dimensional algebra over k, let $\rho \in A \otimes A$ and suppose that s is a linear automorphism of A. Let A^* be the dual coalgebra of A. Then the following are equivalent:*

a) *(A, ρ, s) is a quantum algebra over k.*
b) *(A^*, b_ρ, s^*) is a strict quantum coalgebra over k.*

□

A little more can be squeezed from a proof of the proposition.

COROLLARY 1. *Suppose that (A, ρ, s) is any quantum algebra over k. Then (A^o, b, s^o) is a strict quantum coalgebra over k, where $b(a^o, b^o) = (a^o \otimes b^o)(\rho)$ for all $a^o, b^o \in A^o$.*

□

The strict quantum coalgebra (A^o, b, s^o) of Corollary 1 is called the *dual quantum coalgebra of* (A, ρ, s). The dual quantum coalgebra of the quantum algebra of Example 1 is a basic example of a (strict) quantum coalgebra.

EXAMPLE 7. *Let $q \in k^\star$. Then $(\mathrm{C}_2(k), b, S)$ is a quantum coalgebra over k where*

$$b(e_1^1, e_1^1) = q^{-1} = b(e_2^2, e_2^2), \quad b(e_1^1, e_2^2) = q = b(e_2^2, e_1^1), \quad b(e_2^1, e_1^2) = q^{-1} - q^3$$

and $b(e_j^i, e_m^\ell) = 0$ otherwise, and

$$S(e_1^1) = e_2^2, \quad S(e_2^2) = e_1^1, \quad S(e_2^1) = -q^2 e_2^1 \text{ and } S(e_1^2) = -q^{-2} e_1^2.$$

Also see [**11**, Section 8].

Just as finite-dimensional quasitriangular Hopf algebras give rise to quantum algebras, it is easy to see, following the discussion of [**12**, Section 7.3] for example, that:

EXAMPLE 8. *Let (A, β) be a coquasitriangular Hopf algebra with antipode s over the field k. Then (A, β, s) is a quantum coalgebra over k.*

The notion of oriented quantum coalgebra is introduced in [**8**, Section 4]. Strict oriented quantum coalgebras form an important class of oriented quantum coalgebras. A *strict oriented quantum coalgebra over k* is a quadruple $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$, where C is a coalgebra over k, $b : C \times C \longrightarrow k$ is an invertible bilinear form and $T_{\mathsf{d}}, T_{\mathsf{u}}$ are commuting coalgebra automorphisms of C, such that

(qc.1) $b(c_{(1)}, T_{\mathsf{u}}(d_{(2)}))b^{-1}(T_{\mathsf{d}}(c_{(2)}), d_{(1)}) = \epsilon(c)\epsilon(d)$ and
$b^{-1}(T_{\mathsf{d}}(c_{(1)}), d_{(2)})b(c_{(2)}, T_{\mathsf{u}}(d_{(1)})) = \epsilon(c)\epsilon(d)$,

(qc.2) $b(c,d) = b(T_{\mathsf{d}}(c), T_{\mathsf{d}}(d)) = b(T_{\mathsf{u}}(c), T_{\mathsf{u}}(d))$ and

(qc.3) $b(c_{(1)}, d_{(1)})b(c_{(2)}, e_{(1)})b(d_{(2)}, e_{(2)}) = b(c_{(2)}, d_{(2)})b(c_{(1)}, e_{(2)})b(d_{(1)}, e_{(1)})$

for all $c, d, e \in C$. An *oriented quantum coalgebra over* k is a quadruple $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$, where C is a coalgebra over k, $b : C{\times}C \longrightarrow k$ is an invertible bilinear form and T is a coalgebra automorphism of C with respect to $\{b, b^{-1}\}$, such that (qc.1)–(qc.3) hold. Generally if C, D are coalgebras over k and $\mathcal{S}$ is a set of bilinear forms $b : D{\times}D \longrightarrow k$, then a linear map (respectively isomorphism) $T : C \longrightarrow D$ is a *coalgebra map* (respectively *isomorphism*) *with respect to* $\mathcal{S}$ if

$$b(T(c_{(1)}), d)b'(T(c_{(2)}), e) = b(T(c)_{(1)}, d)b'(T(c)_{(2)}, e)$$

and

$$b(d, T(c_{(1)}))b'(e, T(c_{(2)})) = b(d, T(c)_{(1)})b'(e, T(c)_{(2)})$$

for all $b, b' \in \mathcal{S}$, $c \in C$ and $d, e \in D$. When $C = D$ and T is a coalgebra isomorphism with respect to $\mathcal{S}$ then T is called a *coalgebra automorphism of* C *with respect to* $\mathcal{S}$.

An oriented quantum coalgebra $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is *standard* if $T_{\mathsf{d}} = 1_C$ and is *balanced* if $T_{\mathsf{d}} = T_{\mathsf{u}}$. In the balanced case we write (C, b, T) for (C, b, T, T). A *morphism of oriented quantum coalgebras* $f : (C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (C', b', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ is a coalgebra map $f : C \longrightarrow C'$ which satisfies $b(c,d) = b'((f(c), f(d))$ for all $c, d \in C$ and $T'_{\mathsf{d}} \circ f = f \circ T_{\mathsf{d}}$, $T'_{\mathsf{u}} \circ f = f \circ T_{\mathsf{u}}$. Oriented quantum coalgebras together with their morphisms under composition form a monoidal category.

As remarked in [**9**, Section 3], the notions of oriented quantum algebra and strict oriented quantum coalgebra are dual. We state here more formally:

PROPOSITION 2. *Suppose that A is a finite-dimensional algebra over k, $\rho \in A{\otimes}A$ and $t_{\mathsf{d}}, t_{\mathsf{u}}$ are commuting linear automorphisms of A. Let A^* be the dual coalgebra of A. Then the following are equivalent:*

a) *$(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is an oriented quantum algebra over k.*
b) *$(A^*, b_\rho, t^*_{\mathsf{d}}, t^*_{\mathsf{u}})$ is a strict oriented quantum coalgebra over k.*

□

Moreover:

COROLLARY 2. *Suppose that $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is any oriented quantum algebra over k. Then $(A^o, b, t^o_{\mathsf{d}}, t^o_{\mathsf{u}})$ is a strict oriented quantum coalgebra over k, where $b(a^o, b^o) = (a^o{\otimes}b^o)(\rho)$ for all $a^o, b^o \in A^o$.*

□

The strict oriented quantum coalgebra $(A^o, b, t^o_{\mathsf{d}}, t^o_{\mathsf{d}})$ of Corollary 2 is called the *dual oriented quantum coalgebra of* $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$. The duals of the strict quantum algebras of Example 3 form a rather extensive family of balanced strict oriented quantum coalgebras.

EXAMPLE 9. *Suppose $n \geq 2$ and $bc, x \in k^\star$. Suppose that $\{\rho^{\imath\,\ell}_{\jmath\,m}\}_{1\leq \imath,\jmath\leq n} \subseteq k$ and $\{\omega_\imath\}_{1\leq\imath\leq n} \subseteq k^\star$ satisfy conditions a)–d) and e) respectively of Example 3. Then $(\mathrm{C}_n(k), b, T)$ is a strict balanced oriented quantum coalgebra over k, where $b(e^\imath_\jmath, e^\ell_m) = \rho^{\imath\,\ell}_{\jmath\,m}$ for all $1 \leq \imath, \jmath, \ell, m \leq n$ and $T(e^\imath_\jmath) = (\omega_\imath/\omega_\jmath)e^\imath_\jmath$ for all $1 \leq \imath, \jmath \leq n$.*

Observe that the quantum coalgebra $(\mathrm{C}_2(k), b, S)$ of Example 7 has a strict oriented balanced quantum coalgebra structure $(\mathrm{C}_2(k), b, T)$ which is a special case of the previous example with $\omega_1 = q^{-1}$ and $\omega_2 = -q$. Note that $S \circ T = T \circ S$ and $T^2 = S^{-2}$.

We end this section with a result on coalgebra automorphisms with respect to a set of bilinear forms which will be useful for the proof of Theorem 4 of Section 7.2. Let C be a coalgebra over k and suppose that $\mathcal{S}$ is a set of bilinear forms $b : C \times C \longrightarrow k$. The set of linear automorphisms T of C which satisfy (qc.2) for all $b \in \mathcal{S}$ is easily seen to be a subgroup of the multiplicative group of all linear automorphisms of C.

LEMMA 1. *Let C be a coalgebra over the field k and suppose that $\mathcal{S}$ is a set of bilinear forms $b : C \times C \longrightarrow k$.*

a) *The set of coalgebra automorphisms T of C with respect to $\mathcal{S}$ which satisfy (qc.2) for all $b \in \mathcal{S}$ form a subgroup $\mathcal{G}(C, \mathcal{S})$ of the group of linear automorphisms of C under composition.*

b) *The equations*

$$b(T^{u+\ell}(c_{(1)}), d)b'(T^{v+\ell}(c_{(2)}), e) = b(T^u(T^\ell(c)_{(1)}), d)b'(T^v(T^\ell(c)_{(2)}), e)$$

and

$$b(d, T^{u+\ell}(c_{(1)}))b'(e, T^{v+\ell}(c_{(2)})) = b(d, T^u(T^\ell(c)_{(1)}))b'(e, T^v(T^\ell(c)_{(2)}))$$

hold for all $b, b' \in \mathcal{S}$, for all $T \in \mathcal{G}(C, \mathcal{S})$, for all integers u, v, ℓ and $c, d, e \in C$.

PROOF: It is clear that the identity map of C lies in $\mathcal{G}(C, \mathcal{S})$. Suppose that $T, U \in \mathcal{G}(C, \mathcal{S})$. To complete the proof of part a) we need only show that $T^{-1} \circ U \in \mathcal{G}(C, \mathcal{S})$. For all $b, b' \in S$ and $c, d, e \in C$ observe that

$$\begin{aligned}
& b(T^{-1}(U(c_{(1)})), d)b'(T^{-1}(U(c_{(2)})), e) \\
&= b(U(c_{(1)}), T(d))b'(U(c_{(2)}), T(e)) \\
&= b(U(c)_{(1)}, T(d))b'(U(c)_{(2)}, T(e)) \\
&= b(T(T^{-1}(U(c)))_{(1)}, T(d))b'(T(T^{-1}(U(c)))_{(2)}, T(e)) \\
&= b(T(T^{-1}(U(c))_{(1)}), T(d))b'(T(T^{-1}(U(c))_{(2)}), T(e)) \\
&= b(T^{-1}(U(c))_{(1)}, d)b'(T^{-1}(U(c)_{(2)}, e)
\end{aligned}$$

and likewise

$$b(d, T^{-1}(U(c_{(1)})))b'(e, T^{-1}(U(c_{(2)}))) = b(d, T^{-1}(U(c))_{(1)})b'(e, T^{-1}(U(c))_{(2)}).$$

Therefore $T^{-1} \circ U \in \mathcal{G}(C, \mathcal{S})$. Since $b(T^{u+\ell}(c), d) = b(T^\ell(c), T^{-u}(d))$ and $b(d, T^{u+\ell}(c)) = b(T^{-u}(d), T^\ell(c))$ and for all integers u, ℓ and $c, d, e \in C$, part b) follows from part a). □

4. A Basic Relationship Between Oriented and Unoriented Quantum Algebra Structures

Suppose that (A, ρ, s) is a quantum algebra over k. Then $(A, \rho, 1_A, s^{-2})$ is a standard oriented quantum algebra over k by virtue of Example 4. We have seen that not every oriented quantum algebra is of this form in our discussion following

Example 4. The main purpose of this section is to show that a quantum algebra can be associated with an oriented quantum algebra in a natural way.

Let $(A, \rho, 1_A, t)$ be a standard oriented quantum algebra over k, let $\mathcal{A} = A \oplus A^{op}$ be the direct product of A and A^{op}, and let $\pi : \mathcal{A} \longrightarrow A$ be the projection onto the first factor. We will construct a quantum algebra $(\mathcal{A}, \boldsymbol{\rho}, \mathbf{s})$ on $\mathcal{A}$ such that $\pi : (\mathcal{A}, \rho, 1_{\mathcal{A}}, \mathrm{s}^{-2}) \longrightarrow (A, \rho, 1_A, t)$ is a morphism of oriented quantum algebras.

Let $\overline{(\ )}$ denote the linear involution of $\mathcal{A}$ which exchanges the direct summands of $\mathcal{A}$. Thus $\overline{a \oplus b} = b \oplus a$ for all $a, b \in A$. We regard A as a subspace of $\mathcal{A}$ by the identification $a = a \oplus 0$ for all $a \in A$. Therefore $\overline{a} = 0 \oplus a$ and every element of $\mathcal{A}$ has a unique decomposition of the form $a + \overline{b}$ for some $a, b \in A$. Observe that

$$\overline{(\overline{a})} = a, \quad \overline{ab} = \overline{b}\,\overline{a} \ \text{ and } \ a\overline{b} = 0 = \overline{a}b \tag{1}$$

for all $a, b \in A$. The main result of this section is:

THEOREM 1. *Let $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ be an oriented quantum algebra over the field k, let $\mathcal{A} = A \oplus A^{op}$ be the direct product of A and A^{op} and write $\rho = \sum_{i=1}^{r} a_i \otimes b_i$, $\rho^{-1} = \sum_{j=1}^{s} \alpha_j \otimes \beta_j$. Then:*

a) *$(\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{s})$ is a quantum algebra over k, where*

$$\boldsymbol{\rho} = \sum_{i=1}^{r} (a_i \otimes b_i + \overline{a_i} \otimes \overline{b_i}) + \sum_{j=1}^{s} (\overline{\alpha_j} \otimes \beta_j + \alpha_j \otimes \overline{t_{\mathsf{d}}^{-1} \circ t_{\mathsf{u}}^{-1}(\beta_j)})$$

and $\boldsymbol{s}(a \oplus b) = b \oplus t_{\mathsf{d}}^{-1} \circ t_{\mathsf{u}}^{-1}(a)$ for all $a, b \in A$.

b) *$(\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{t}_{\mathsf{d}}, \boldsymbol{t}_{\mathsf{u}})$ is an oriented quantum algebra over k, $\boldsymbol{t}_{\mathsf{d}}, \boldsymbol{t}_{\mathsf{u}}$ commute with $\boldsymbol{s}$ and $\boldsymbol{t}_{\mathsf{d}} \circ \boldsymbol{t}_{\mathsf{u}} = \boldsymbol{s}^{-2}$, where $\boldsymbol{t}_{\mathsf{d}}(a \oplus b) = t_{\mathsf{d}}(a) \oplus t_{\mathsf{d}}(b)$ and $\boldsymbol{t}_{\mathsf{u}}(a \oplus b) = t_{\mathsf{u}}(a) \oplus t_{\mathsf{u}}(b)$ for all $a, b \in A$.*

c) *The projection $\pi : \mathcal{A} \longrightarrow A$ onto the first factor determines a morphism $\pi : (\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{t}_{\mathsf{d}}, \boldsymbol{t}_{\mathsf{u}}) \longrightarrow (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ of oriented quantum algebras.*

PROOF: This result was announced as [**16**, Theorem 2] and the proof here was also given in that paper. We repeat the proof here for the reader's convenience and to connect it to a proof of Theorem 3.

Part b) is a straightforward calculation which is left to the reader and part c) follows by definitions. As for part a) we may assume that $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}}) = (A, \rho, 1_A, t)$ is standard. In this case

$$\boldsymbol{\rho} = \sum_{i=1}^{r} (a_i \otimes b_i + \overline{a_i} \otimes \overline{b_i}) + \sum_{j=1}^{s} (\overline{\alpha_j} \otimes \beta_j + \alpha_j \otimes \overline{t^{-1}(\beta_j)}) \quad \text{and} \quad \boldsymbol{s}(a \oplus b) = b \oplus t^{-1}(a)$$

for all $a, b \in A$. Since t is an algebra automorphism of A it follows that t^{-1} is also. Thus $\boldsymbol{s} : \mathcal{A} \longrightarrow \mathcal{A}^{op}$ is an algebra isomorphism. By definition $\boldsymbol{s}(a) = \overline{t^{-1}(a)}$ and $\boldsymbol{s}(\overline{a}) = a$ for all $a \in A$. Since $\rho = (t \otimes t)(\rho)$ it follows that $\rho^{-1} = (t^{-1} \otimes t^{-1})(\rho^{-1})$. At this point it is easy to see that $\boldsymbol{\rho} = (\boldsymbol{s} \otimes \boldsymbol{s})(\boldsymbol{\rho})$, or (QA.2) is satisfied for $\boldsymbol{\rho}$ and $\boldsymbol{s}$. Using the equation $\rho^{-1} = (t^{-1} \otimes t^{-1})(\rho^{-1})$ we calculate

$$(s \otimes 1_{\mathcal{A}})(\boldsymbol{\rho}) = \sum_{i=1}^{r} \left(\overline{t^{-1}(a_i)} \otimes b_i + a_i \otimes \overline{b_i} \right) + \sum_{j=1}^{s} \left(\alpha_j \otimes \beta_j + \overline{\alpha_j} \otimes \overline{\beta_j} \right).$$

Using (1), the equation $(t^{-1} \otimes 1_A)(\rho) = (1_A \otimes t)(\rho)$, which follows by (qa.2), we see that

$$\boldsymbol{\rho}((s \otimes 1_{\mathcal{A}})(\boldsymbol{\rho})) = 1 \otimes 1 + \overline{1} \otimes \overline{1} + \overline{1} \otimes 1 + 1 \otimes \overline{1} = 1_{\mathcal{A}} \otimes 1_{\mathcal{A}} = ((s \otimes 1_{\mathcal{A}})(\boldsymbol{\rho}))\boldsymbol{\rho}.$$

Therefore $\boldsymbol{\rho}$ is invertible and $\boldsymbol{\rho}^{-1} = (\boldsymbol{s}\otimes 1_A)(\boldsymbol{\rho})$. We have shown that (QA.1) holds for $\boldsymbol{\rho}$ and $\boldsymbol{s}$.

That $\boldsymbol{\rho}$ satisfies (QA.3) is a rather lengthy and interesting calculation. It is a straightforward exercise to see that (QA.3) for $\boldsymbol{\rho}$ is equivalent to a set of eight equations. With the notation convention $(\rho^{-1})_{\imath\jmath} = \rho_{\imath\jmath}^{-1}$ for $1 \le \imath < \jmath \le 3$, this set of eight equations can be rewritten as set of six equations which are:

$$\rho_{1\,2}\rho_{1\,3}\rho_{2\,3} = \rho_{2\,3}\rho_{1\,3}\rho_{1\,2}, \tag{2}$$

$$\rho_{1\,2}\rho_{2\,3}^{-1}\rho_{1\,3}^{-1} = \rho_{1\,3}^{-1}\rho_{2\,3}^{-1}\rho_{1\,2}, \tag{3}$$

$$\rho_{1\,3}^{-1}\rho_{1\,2}^{-1}\rho_{2\,3} = \rho_{2\,3}\rho_{1\,2}^{-1}\rho_{1\,3}^{-1}, \tag{4}$$

$$\sum_{\ell=1}^{r}\sum_{\jmath,m=1}^{s} a_\ell\alpha_\jmath\otimes\beta_\jmath\alpha_m\otimes t^{-1}(\beta_m)b_\ell = \sum_{\jmath,m=1}^{s}\sum_{\ell=1}^{r}\alpha_\jmath a_\ell\otimes\alpha_m\beta_\jmath\otimes b_\ell t^{-1}(\beta_m), \tag{5}$$

$$\sum_{\jmath,m=1}^{s}\sum_{\ell=1}^{r}\alpha_\jmath a_\ell\otimes\alpha_m t^{-1}(\beta_\jmath)\otimes b_\ell\beta_m = \sum_{\ell=1}^{r}\sum_{\jmath,m=1}^{s} a_\ell\alpha_\jmath\otimes t^{-1}(\beta_\jmath)\alpha_m\otimes\beta_m b_\ell \tag{6}$$

and

$$\sum_{\jmath,\ell=1}^{s}\sum_{\ell=1}^{r}\alpha_\jmath\alpha_\ell\otimes a_m t^{-1}(\beta_\jmath)\otimes b_m t^{-1}(\beta_\ell) = \sum_{\ell,\jmath=1}^{s}\sum_{m=1}^{r}\alpha_\ell\alpha_\jmath\otimes t^{-1}(\beta_\jmath)a_m\otimes t^{-1}(\beta_\ell)b_m. \tag{7}$$

By assumption (2) holds. Since $\rho_{\imath\jmath}$ is invertible and $(\rho_{\imath\jmath})^{-1} = (\rho^{-1})_{\imath\jmath} = \rho_{\imath\jmath}^{-1}$, equations (3)–(4) hold since (2) does.

We note that t^{-1} is an algebra automorphism of A and $\rho^{-1} = (t^{-1}\otimes t^{-1})(\rho^{-1})$. Thus applying $1_A\otimes t^{-1}\otimes 1_A$ to both sides of the equation of (5) we see that (5) and (6) are equivalent; applying $t^{-1}\otimes 1_A\otimes 1$ to both sides of (7) we see that (7) is equivalent to $\rho_{2\,3}\rho_{1\,2}^{-1}\rho_{1\,3}^{-1} = \rho_{1\,3}^{-1}\rho_{1\,2}^{-1}\rho_{2\,3}$, a consequence of (2). To complete the proof of part a) we need only show that (5) holds.

By assumption $(1_A\otimes t)(\rho)$ and ρ^{-1} are inverses in $A\otimes A^{op}$. Thus ρ and $(1_A\otimes t^{-1})(\rho)$ are inverses in $A\otimes A^{op}$ as $1_A\otimes t^{-1}$ is an algebra endomorphism of

$A \otimes A^{op}$. Recall that ρ^{-1} satisfies (QA.3). Therefore

$$\begin{aligned}
&\sum_{\jmath,m=1}^{s}\sum_{\ell=1}^{r}\alpha_\jmath a_\ell \otimes \alpha_m\beta_\jmath \otimes b_\ell t^{-1}(\beta_m) \\
&= \sum_{v,\ell=1}^{r}\sum_{u,\jmath,m=1}^{s}(a_v\alpha_u)\alpha_\jmath a_\ell \otimes \alpha_m\beta_\jmath \otimes b_\ell t^{-1}(\beta_m)(t^{-1}(\beta_u)b_v) \\
&= \sum_{v,\ell=1}^{r}\sum_{u,\jmath,m=1}^{s}a_v(\alpha_u\alpha_\jmath)a_\ell \otimes \alpha_m\beta_\jmath \otimes b_\ell t^{-1}(\beta_m\beta_u)b_v \\
&= \sum_{v,\ell=1}^{r}\sum_{u,\jmath,m=1}^{s}a_v(\alpha_\jmath\alpha_u)a_\ell \otimes \beta_\jmath\alpha_m \otimes b_\ell t^{-1}(\beta_u\beta_m)b_v \\
&= \sum_{v,\ell=1}^{r}\sum_{u,\jmath,m=1}^{s}a_v\alpha_\jmath(\alpha_u a_\ell) \otimes \beta_\jmath\alpha_m \otimes (b_\ell t^{-1}(\beta_u))t^{-1}(\beta_m)b_v \\
&= \sum_{v=1}^{r}\sum_{\jmath,m=1}^{s}a_v\alpha_\jmath \otimes \beta_\jmath\alpha_m \otimes t^{-1}(\beta_m)b_v.
\end{aligned}$$

which establishes (5). □

Denote by $\mathcal{C}_q$ the category whose objects are quintuples $(A, \rho, s, t_{\mathsf{d}}, t_{\mathsf{u}})$, where (A, ρ, s) is a quantum algebra over k and $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is an oriented quantum algebra over k such that $t_{\mathsf{d}}, t_{\mathsf{u}}$ commute with s and $t_{\mathsf{d}} \circ t_{\mathsf{u}} = s^{-2}$, and whose morphisms $f : (A, \rho, s, t_{\mathsf{d}}, t_{\mathsf{u}}) \longrightarrow (A', \rho', s', t'_{\mathsf{d}}, t'_{\mathsf{u}})$ are algebra maps $f : A \longrightarrow A'$ which determine morphisms $f : (A, \rho, s) \longrightarrow (A', \rho', s')$ and $f : (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}}) \longrightarrow (A', \rho', t'_{\mathsf{d}}, t'_{\mathsf{u}})$. The construction $(\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{s}, \boldsymbol{t_{\mathsf{d}}}, \boldsymbol{t_{\mathsf{d}}})$ of Theorem 1 is a cofree object of $\mathcal{C}_q$. Let $\pi : \mathcal{A} \longrightarrow A$ be the projection onto the first factor.

PROPOSITION 3. *Let $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ be an oriented quantum algebra over the field k. Then the pair $((\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{s}, \boldsymbol{t_{\mathsf{d}}}, \boldsymbol{t_{\mathsf{u}}}), \pi)$ satisfies the following properties:*

a) *$(\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{s}, \boldsymbol{t_{\mathsf{d}}}, \boldsymbol{t_{\mathsf{u}}})$ is an object of $\mathcal{C}_q$ and $\pi : (\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{t_{\mathsf{d}}}, \boldsymbol{t_{\mathsf{u}}}) \longrightarrow (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is a morphism of oriented quantum algebras.*

b) *Suppose that $(A', \rho', s', t'_{\mathsf{d}}, t'_{\mathsf{u}})$ is an object of $\mathcal{C}_q$ and suppose that $f : (A', \rho', t'_{\mathsf{d}}, t'_{\mathsf{u}}) \longrightarrow (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is a morphism of oriented quantum algebras. Then there is a morphism $F : (A', \rho', s', t'_{\mathsf{d}}, t'_{\mathsf{u}}) \longrightarrow (\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{s}, \boldsymbol{t_{\mathsf{d}}}, \boldsymbol{t_{\mathsf{u}}})$ uniquely determined by $\pi \circ F = f$.*

PROOF: We have shown part a). Let $f : (A', \rho, t'_{\mathsf{d}}, t'_{\mathsf{u}}) \longrightarrow (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ be a morphism of oriented quantum algebras. To show part b) we first suppose that $F : (A', \rho', s', t'_{\mathsf{d}}, t'_{\mathsf{u}}) \longrightarrow (\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{s}, \boldsymbol{t_{\mathsf{d}}}, \boldsymbol{t_{\mathsf{u}}})$ is a morphism which satisfies $\pi \circ F = f$. Now there are linear maps $g, h : A' \longrightarrow A$ such that $F(x) = g(x) \oplus h(x)$ for all $x \in A'$. Since $\pi \circ F = f$ it follows that $g = f$. Since $s \circ F = F \circ s'$ it follows that $h = g \circ s' = f \circ s'$. Thus $F(x) = f(x) \oplus f(s'(x))$ for all $x \in A'$ which establishes the uniqueness assertion of part b).

To establish the existence assertion of part b), we consider the algebra homomorphism $F : A' \longrightarrow A$ defined by $F(x) = f(x) \oplus f(s'(x))$ for all $x \in A'$. Since $f : (A', \rho', t'_{\mathsf{d}}, t'_{\mathsf{u}}) \longrightarrow (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is a morphism $f \circ t'_{\mathsf{d}} = t_{\mathsf{d}} \circ f$ and $f \circ t'_{\mathsf{u}} = t_{\mathsf{u}} \circ f$.

Therefore

$$\begin{aligned} \boldsymbol{s}\circ F(x) &= f(s'(x))\oplus(t_{\mathsf{d}}^{-1}\circ t_{\mathsf{u}}^{-1}\circ f)(x) \\ &= f(s'(x))\oplus(f\circ t_{\mathsf{d}}'^{-1}\circ t_{\mathsf{u}}'^{-1})(x) \\ &= f(s'(x))\oplus f((s'^2(x)) \\ &= F\circ s'(x) \end{aligned}$$

for all $x \in A'$ which shows that $\boldsymbol{s}\circ F = F\circ s'$. Since t_{d}' and s' commute the calculation

$$\begin{aligned} \boldsymbol{t}_d\circ F(x) &= t_{\mathsf{d}}(f(x))\oplus t_{\mathsf{d}}(f(s'(x))) \\ &= f(t_{\mathsf{d}}'(x))\oplus f(t_{\mathsf{d}}'(s'(x))) \\ &= f(t_{\mathsf{d}}'(x))\oplus f(s'(t_{\mathsf{d}}'(x))) \\ &= F\circ t_{\mathsf{d}}'(x) \end{aligned}$$

for all $x \in A'$ establishes $\boldsymbol{t}_d\circ F = F\circ t_{\mathsf{d}}'$. Likewise $\boldsymbol{t}_u\circ F = F\circ t_{\mathsf{u}}'$.

To complete the proof that $F : (A', \rho', s', t_{\mathsf{d}}', t_{\mathsf{u}}') \longrightarrow (\mathcal{A}, \boldsymbol{\rho}, \boldsymbol{s}, \boldsymbol{T}_d, \boldsymbol{T}_d)$ is a morphism, and thus to complete the proof of the proposition, we need only show that $\boldsymbol{\rho} = (F\oplus F)(\boldsymbol{\rho})$. Since $f : (A', \rho', t_{\mathsf{d}}', t_{\mathsf{u}}') \longrightarrow (A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ is a morphism of oriented quantum algebras $\rho = (f\otimes f)(\rho')$ and thus $\rho^{-1} = (f\oplus f)(\rho'^{-1})$. Now $f\circ s'^2 = t_{\mathsf{d}}^{-1}\circ t_{\mathsf{u}}^{-1}\circ f$ follows from the hypothesis of part b). Write $\rho = \sum_{\imath=1}^{r} a_\imath\otimes b_\imath$ and $\rho' = \sum_{\imath'=1}^{r'} a'_{\imath'}\otimes b_{\imath'}$. Using the fact that (A', ρ', s') is a quantum algebra we can now calculate

$$\begin{aligned} (F\otimes F)(\rho') &= \sum_{\imath'=1}^{r'} F(a'_{\imath'})\otimes F(b'_{\imath'}) \\ &= \sum_{\imath'=1}^{r'} (f(a'_{\imath'})\oplus f(s'(a'_{\imath'})))\otimes(f(b'_{\imath'})\oplus f(s'(b'_{\imath'}))) \\ &= \sum_{\imath'=1}^{r'} \left(f(a'_{\imath'}) + \overline{f(s'(a'_{\imath'}))}\right)\otimes\left(f(b'_{\imath'}) + \overline{f(s'(b'_{\imath'}))}\right) \\ &= \sum_{\imath'=1}^{r'} \left(f(a'_{\imath'})\otimes f(b'_{\imath'}) + \overline{f(s'(a'_{\imath'}))}\otimes\overline{f(s'(b'_{\imath'}))}\right) \\ &\quad + \sum_{\imath'=1}^{r'} \left(\overline{f(s(a'_{\imath'}))}\otimes f(b'_{\imath'}) + f(a'_{\imath'})\otimes\overline{f(s'(b'_{\imath'}))}\right) \\ &= \sum_{\imath'=1}^{r'} \left(f(a'_{\imath'})\otimes f(b'_{\imath'}) + \overline{f(a'_{\imath'})}\otimes\overline{f(b'_{\imath'})}\right) \\ &\quad + \sum_{\imath'=1}^{r'} \left(\overline{f(s(a'_{\imath'}))}\otimes f(b'_{\imath'}) + f(s'(a'_{\imath'}))\otimes\overline{f(s'^2(b'_{\imath'}))}\right) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\imath'=1}^{r'} \Big(f(a'_{\imath'}) \otimes f(b'_{\imath'}) + \overline{f(a'_{\imath'})} \otimes \overline{f(b'_{\imath'})} \Big) \\
&\quad + \sum_{\imath'=1}^{r'} \Big(\overline{f(s(a'_{\imath'}))} \otimes f(b'_{\imath'}) + f(s'(a'_{\imath'})) \otimes \overline{t_{\mathsf{d}}^{-1} \circ t_{\mathsf{u}}^{-1}(f(b'_{\imath'}))} \Big) \\
&= \sum_{\imath=1}^{r} \big(a_\imath \otimes b_\imath + \overline{a_\imath} \otimes \overline{b_\imath} \big) + \sum_{\jmath=1}^{s} \Big(\overline{\alpha_\jmath} \otimes \beta_\jmath + \alpha_\jmath \otimes \overline{t_{\mathsf{d}}^{-1} \circ t_{\mathsf{u}}^{-1}(\beta_\jmath)} \Big) \\
&= \boldsymbol{\rho}.
\end{aligned}
$$

□

5. General Results for Oriented Quantum Coalgebras

In this section we develop some of the basic theory of oriented quantum coalgebras. Our discussion parallels that of [**11**, Sections 4 and 5] to a good extent. Proofs of most assertions made in this section can be obtained by modifying the proofs of corresponding statements in [**11**] about quantum coalgebras. Thus we shall tend to omit many details here.

Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ be an oriented quantum coalgebra over the field k and let $b', b'' : C \times C^{cop} \longrightarrow k$ be the bilinear forms defined by $b'(c,d) = b(c, T_{\mathsf{u}}(d))$ and $b''(c,d) = b^{-1}(T_{\mathsf{d}}(c), d)$ for all $c, d \in C$. Then the two equations of (qc.1) may be viewed as technical formulations of the statements b'' is a left inverse for b' and b'' is a right inverse for b'. When C is finite-dimensional the two equations of (qc.1) are equivalent. Thus in the finite-dimensional case, axiom (qc.1) for oriented quantum coalgebra can be simplified.

A straightforward calculation shows that $(C^{cop}, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is an oriented quantum coalgebra over k. Let $T = T_{\mathsf{d}}$ or $T = T_{\mathsf{u}}$. Since T^{-1} is a coalgebra automorphism of C with respect to $\{b, b^{-1}\}$, by part a) of Lemma 1 and the equation $b^{-1}(T(c), T(d)) = b^{-1}(c,d)$ for all $c, d \in C$, it follows that $(C, b^{-1}, T_{\mathsf{d}}^{-1}, T_{\mathsf{u}}^{-1})$ is an oriented quantum coalgebra over k. See the proof of the corresponding statement for quantum coalgebras given in [**11**, Section 4.2]. Let $b^{op} : C \times C \longrightarrow k$ be the bilinear form defined by $b^{op}(c,d) = b(d,c)$ for all $c, d \in C$. Then $(C, b^{op}, T_{\mathsf{u}}, T_{\mathsf{d}})$ is an oriented quantum coalgebra over k as well.

Let K be a field extension of k. Then $(C \otimes K, b \otimes 1_{K \otimes K}, T_d \otimes 1_K, T_{\mathsf{u}} \otimes 1_K)$ is an oriented quantum coalgebra over K, where $b \otimes 1_{K \otimes K}(c \otimes \alpha, d \otimes \beta) = \alpha\beta b(c,d)$ for all $c, d \in C$ and $\alpha, \beta \in K$. Suppose that $(C', b', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ is also an oriented quantum coalgebra over k. Then $(C \otimes C', b'', T_{\mathsf{d}} \otimes T'_{\mathsf{d}}, T_{\mathsf{u}} \otimes T'_{\mathsf{u}})$ is an oriented quantum coalgebra over k, called the *tensor product of oriented quantum coalgebras over* k, where $b''(c \otimes c', d \otimes d') = b(c,d)b'(c',d')$ for all $c, d \in C$ and $c', d' \in C'$.

An *oriented quantum subcoalgebra of* $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is an oriented quantum coalgebra $(D, b', T'_{\mathsf{d}}, T'_{\mathsf{u}})$, where D is a subcoalgebra of C and the inclusion $\imath : D \longrightarrow C$ determines a morphism $\imath : (D, b', T'_{\mathsf{d}}, T'_{\mathsf{u}}) \longrightarrow (C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$. In this case $b' = b|_{D \times D}$, $T_{\mathsf{d}}(D) = D = T_{\mathsf{u}}(D)$ and $T'_{\mathsf{d}} = T_{\mathsf{d}}|_D$, $T'_{\mathsf{u}} = T_{\mathsf{u}}|_D$. Conversely, if D is a subcoalgebra of C and $T_{\mathsf{d}}(D) = D = T_{\mathsf{u}}(D)$, then $(D, b_{D \times D}, T_{\mathsf{d}}|_D, T_{\mathsf{u}}|_D)$ is an oriented quantum subcoalgebra of $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$.

Let I be a coideal of C which satisfies $T_{\mathsf{d}}(I) = I = T_{\mathsf{u}}(I)$ and $b(I, C) = (0) = b(C, I)$. Then the quotient C/I has a unique oriented quantum coalgebra structure $(C/I, \overline{b}, \overline{T}_{\mathsf{d}}, \overline{T}_{\mathsf{u}})$, which we refer to as a *quotient oriented quantum*

coalgebra structure, such that the projection $\pi : C \longrightarrow C/I$ induces a morphism $\pi : (C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (C/I, \overline{b}, \overline{T}_{\mathsf{d}}, \overline{T}_{\mathsf{u}})$.

Let I be the sum of the coideals J of C such that $T_{\mathsf{d}}(J) = J = T_{\mathsf{u}}(J)$ and $b(J, C) = (0) = b(C, J)$. Then I is a coideal of C which satisfies $T_{\mathsf{d}}(I) = I = T_{\mathsf{u}}(I)$ and $b(I, C) = (0) = b(C, I)$. Set $C_r = C/I$. The quotient oriented quantum coalgebras structure $(C_r, b_r, T_{r\,\mathsf{d}}, T_{r\,\mathsf{u}})$ is the coalgebra counterpart of the minimal oriented quantum subalgebra $(A_\rho, \rho, t_{\mathsf{d}}|_{A_\rho}, t_{\mathsf{u}}|_{A_\rho})$ of an oriented quantum algebra $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ over k. Observe that if J is a coideal of C_r such that $T_{r\,\mathsf{d}}(J) = J = T_{r\,\mathsf{u}}(J)$ and $b_r(J, C_r) = (0) = b_r(C_r, J)$ then $J = (0)$.

Recall that a bilinear form $\beta : V \times V \longrightarrow k$ define for a vector space over k is *left* (respectively *right*) *non-singular* if $\beta_{(\ell)}$ (respectively $\beta_{(r)}$) is one-one. If b is either left non-singular or right non-singular then $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is strict.

LEMMA 2. *Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ be an oriented quantum coalgebra over the field k and suppose that b is either left non-singular or is right non-singular. Then T_{d} and T_{u} are coalgebra automorphisms of C.*

PROOF: Consider the linear map $b_{(\ell)} \otimes b_{(\ell)} : C \otimes C \longrightarrow C^* \otimes C^*$ and regard $C^* \otimes C^*$ as a subspace of $(C \otimes C)^*$ by $(c^* \otimes d^*)(c \otimes d) = c^*(c)d^*(d)$ for all $c^*, d^* \in C^*$ and $c, d \in C$. Let $T = T_{\mathsf{d}}$ or $T = T_{\mathsf{u}}$. Then

$$b(d, T(c_{(1)}))b(e, T(c_{(2)})) = b(d, T(c)_{(1)})b(e, T(c)_{(2)})$$

for all $d, c, e \in C$ which holds if and only if

$$b_{(\ell)} \otimes b_{(\ell)}(T(c_{(1)}) \otimes T(c_{(2)})) = b_{(\ell)} \otimes b_{(\ell)}(T(c)_{(1)} \otimes T(c)_{(2)})$$

for all $c \in C$. Since $\epsilon \circ T = \epsilon$, it follows that T is a coalgebra automorphism of C if $b_{(\ell)}$ is one-one. Likewise T is a coalgebra automorphism of C if $b_{(r)}$ is one-one. □

Oriented quantum coalgebra structures can be pulled back just as quantum coalgebra structures can be pulled back.

THEOREM 2. *Suppose that $\pi : C \longrightarrow C'$ is an onto map of coalgebras over the field k and suppose that $(C', b', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ is an oriented quantum coalgebra structure on C. Then there exists an oriented quantum coalgebra structure $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ on C such that $\pi : (C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (C', b', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ is a morphism.*

PROOF: The proof boils down to finding commuting linear automorphisms $T_{\mathsf{d}}, T_{\mathsf{u}}$ of C which satisfies $T'_{\mathsf{d}} \circ \pi = \pi \circ T_{\mathsf{d}}$ and $T'_{\mathsf{u}} \circ \pi = \pi \circ T_{\mathsf{u}}$. This is easy enough to do. The reader may want to refer to the proof of the corresponding result for quantum coalgebras [**11**, Theorem 2]. □

By [**12**, Proposition 1.1.1], for example, every finite-dimensional coalgebra over k is the quotient of $\mathrm{C}_n(k)$ for some $n \geq 1$. Thus as a corollary to Theorem 2:

COROLLARY 3. *Every finite-dimensional oriented quantum coalgebra over the field k is the quotient of an oriented quantum coalgebra structure on $\mathrm{C}_n(k)$ for some $n \geq 1$.*

□

There is an analog of [**8**, Proposition 2] for quantum coalgebras.

PROPOSITION 4. *If (C, b, S) is a quantum (respectively strict quantum) coalgebra over k then $(C, b, 1_C, S^{-2})$ is an oriented (respectively strict oriented) quantum coalgebra over k.*

PROOF: Let (C, b, S) be a quantum coalgebra over k. To prove the proposition we need only show that $(C, b, 1_C, S^{-2})$ is an oriented quantum coalgebra over k. Since $S : C \longrightarrow C^{cop}$ is a coalgebra isomorphism with respect to b and (QC.1), (QC.2) hold for S it follows that S^{-2} is a coalgebra automorphism of C with respect to $\{b, b^{-1}\}$. See the proof of Lemma 1. Since (QC.2) holds for S it follows that (qc.2) holds for S^{-2}. Now (QC.3) is (qc.3). Thus to complete the proof we need only show that (qc.1) holds for $T_{\mathtt{d}} = 1_C$ and $T_{\mathtt{d}} = S^{-2}$. The calculation

$$\begin{aligned} b(c_{(1)}, S^{-2}(d_{(2)}))b^{-1}(c_{(2)}, d_{(1)}) &= b(S(c_{(1)}), S^{-1}(d_{(2)}))b(S(c_{(2)}), d_{(1)}) \\ &= b(S(c)_{(2)}, S^{-1}(d_{(2)}))b(S(c)_{(1)}, d_{(1)}) \\ &= b^{-1}(S(c)_{(2)}, d_{(2)})b(S(c)_{(1)}, d_{(1)}) \\ &= \epsilon(S(c))\epsilon(d) \\ &= \epsilon(c)\epsilon(d) \end{aligned}$$

for all $c, d \in C$ shows that $b(c_{(1)}, S^{-2}(d_{(2)}))b^{-1}(c_{(2)}, d_{(1)}) = \epsilon(c)\epsilon(d)$ for all $c, d \in C$. Likewise $b^{-1}(c_{(1)}, d_{(2)})b(c_{(2)}, S^{-2}(d_{(1)})) = \epsilon(c)\epsilon(d)$ for all $c, d \in C$. We have established (qc.1) for $T_{\mathtt{d}} = 1_C$ and $T_{\mathtt{u}} = S^{-2}$. □

By virtue of the preceding proposition every quantum coalgebra over k has the structure of a standard oriented quantum coalgebra. Every oriented quantum coalgebra over k does also by the analog of [**8**, Proposition 1].

PROPOSITION 5. *If $(C, b, T_{\mathtt{d}}, T_{\mathtt{u}})$ is an oriented quantum coalgebra over k then $(C, b, T_{\mathtt{d}} \circ T_{\mathtt{u}}, 1_C)$ and $(C, b, 1_C, T_{\mathtt{d}} \circ T_{\mathtt{u}})$ are also.*

PROOF: Let $(C, b, T_{\mathtt{d}}, T_{\mathtt{u}})$ be an oriented quantum coalgebra over k. By Lemma 1 the composition $T_{\mathtt{d}} \circ T_{\mathtt{u}}$ is a coalgebra automorphism of C with respect to $\{b, b^{-1}\}$. The proof boils down to showing that (qc.1) holds for $(C, b, T_{\mathtt{d}} \circ T_{\mathtt{u}}, 1_C)$ and $(C, b, 1_C, T_{\mathtt{d}} \circ T_{\mathtt{u}})$. To show that (qc.1) holds for $(C, b, T_{\mathtt{d}} \circ T_{\mathtt{u}}, 1_C)$ we note that

$$\begin{aligned} & b(c_{(1)}, d_{(2)})b^{-1}(T_{\mathtt{d}} \circ T_{\mathtt{u}}(c_{(2)}), d_{(1)}) \\ &= b(T_{\mathtt{u}}(c_{(1)}), T_{\mathtt{u}}(d_{(2)}))b^{-1}(T_{\mathtt{u}}(c_{(2)}), T_{\mathtt{d}}^{-1}(d_{(1)})) \\ &= b(T_{\mathtt{u}}(c)_{(1)}, T_{\mathtt{u}}(d_{(2)}))b^{-1}(T_{\mathtt{u}}(c)_{(2)}, T_{\mathtt{d}}^{-1}(d_{(1)})) \\ &= b(T_{\mathtt{u}}(c)_{(1)}, T_{\mathtt{u}}(d_{(2)}))b^{-1}(T_{\mathtt{d}}(T_{\mathtt{u}}(c)_{(2)}), d_{(1)}) \\ &= \epsilon(T_{\mathtt{u}}(c))\epsilon(d) \\ &= \epsilon(c)\epsilon(d) \end{aligned}$$

for all $c, d \in C$ and likewise $b^{-1}(T_{\mathtt{d}} \circ T_{\mathtt{u}}(c_{(1)}), d_{(2)})b(c_{(2)}, d_{(1)}) = \epsilon(c)\epsilon(d)$ for all $c, d \in C$. Similar calculations show that (qc.1) holds for $(C, b, 1_C, T_{\mathtt{d}} \circ T_{\mathtt{u}})$ also. The fact that $T_{\mathtt{d}}$ and $T_{\mathtt{u}}$ commute is used in the latter. □

6. A Basic Relationship Between Oriented and Unoriented Quantum Coalgebra Structures

Let $(C, b, T_{\mathtt{d}}, T_{\mathtt{u}})$ be an oriented quantum coalgebra over the field k and let $\mathcal{C} = C \oplus C^{cop}$ be the direct sum of the coalgebras C and C^{cop}. There is a quantum

coalgebra structure $(\mathcal{C}, \boldsymbol{\beta}, \mathbf{S})$ on $\mathcal{C}$ which is accounted for by [**5**, Theorem 1] and there is a coalgebra counterpart of Theorem 1.

Let $\imath : C \longrightarrow \mathcal{C}$ be the one-one map defined by $\imath(c) = c \oplus 0$ for all $c \in C$, make the identification $c = \imath(c)$ for all $c \in C$ and define $\overline{c \oplus d} = d \oplus c$ for all $c, d \in C$.

THEOREM 3. *Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ be an oriented quantum coalgebra over the field k and let $\mathcal{C} = C \oplus C^{cop}$ be the direct sum of C and C^{cop}. Then:*

a) *$(\mathcal{C}, \boldsymbol{\beta}, \mathbf{S})$ is a quantum coalgebra over k, where $\boldsymbol{\beta}$ is determined by*

$$\boldsymbol{\beta}(c, d) = b(c, d) = \boldsymbol{\beta}(\overline{c}, \overline{d}), \quad \boldsymbol{\beta}(\overline{c}, d) = b^{-1}(c, d),$$
$$\boldsymbol{\beta}(c, \overline{d}) = b^{-1}(c, T^{-2}(d)) \text{ and } \mathbf{S}(c \oplus d) = T_{\mathsf{d}}^{-1} \circ T_{\mathsf{u}}^{-1}(d) \oplus c$$

for all $c, d \in C$.

b) *$(\mathcal{C}, \boldsymbol{\beta}, \mathbf{T}_{\mathsf{d}}, \mathbf{T}_{\mathsf{u}})$ is an oriented quantum coalgebra over k and $\mathbf{T}_{\mathsf{d}}, \mathbf{T}_{\mathsf{u}}$ commute with $\mathbf{S}$, where $\mathbf{T}_{\mathsf{d}}(c \oplus d) = T_{\mathsf{d}}(c) \oplus T_{\mathsf{d}}(d)$ and $\mathbf{T}_{\mathsf{u}}(c \oplus d) = T_{\mathsf{u}}(c) \oplus T_{\mathsf{u}}(d)$ for all $c, d \in C$.*

c) *The inclusion $\imath : C \longrightarrow \mathcal{C}$ induces a morphism of oriented quantum coalgebras $\imath : (C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (\mathcal{C}, \boldsymbol{\beta}, \mathbf{T}_{\mathsf{d}}, \mathbf{T}_{\mathsf{u}})$.*

PROOF: The proofs of parts b) and c) are straightforward and are left to the reader. As for part a), we first note that $(C, b, 1_C, T_{\mathsf{d}} \circ T_{\mathsf{u}})$ is an oriented quantum coalgebra over k by Proposition 5 and that $(C, b, (T_{\mathsf{d}} \circ T_{\mathsf{u}})^{-1})$ is a $(T_{\mathsf{d}} \circ T_{\mathsf{u}})^{-1}$-form structure [**5**, Section 3]. Thus part a) follows by [**5**, Theorem 1]. □

The proof of [**5**, Theorem 1] is conceptually far more difficult than the proof of Theorem 1. The formulation of [**5**, Theorem 1] preceded the definitions of oriented quantum algebra and oriented quantum coalgebra. The motivation for this theorem was to simplify calculation of invariants of 1–1 tangles which arise from certain quantum coalgebras.

Let $\mathcal{C}_{cq}$ be the category whose objects are quintuples $(C, b, S, T_{\mathsf{d}}, T_{\mathsf{u}})$, where (C, b, S) is a quantum coalgebra over k, $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is an oriented quantum coalgebra over k and T_{d}, T_{u} commute with S, and whose morphisms $f : (C, b, S, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (C', b', S', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ are morphisms of quantum coalgebras $f : (C, b, S) \longrightarrow (C', b', S')$ and morphisms of oriented quantum coalgebras $f : (C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (C', b', T'_{\mathsf{d}}, T'_{\mathsf{u}})$. Our construction gives rise to a free object of $\mathcal{C}_{cq}$. The following result, whose proof is left to the reader, is a coalgebra counterpart of Proposition 3.

PROPOSITION 6. *Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ be an oriented quantum coalgebra over the field k. Then the pair $(\imath, (\mathcal{C}, \boldsymbol{\beta}, \boldsymbol{S}, \boldsymbol{T}_{\mathsf{d}}, \boldsymbol{T}_{\mathsf{u}}))$ satisfies the following properties:*

a) *$(\mathcal{C}, \boldsymbol{\beta}, \boldsymbol{S}, \boldsymbol{T}_{\mathsf{d}}, \boldsymbol{T}_{\mathsf{u}})$ is an object of $\mathcal{C}_{cq}$ and $\imath : (C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (\mathcal{C}, \boldsymbol{\beta}, \boldsymbol{T}_{\mathsf{d}}, \boldsymbol{T}_{\mathsf{u}})$ is a morphism of oriented quantum coalgebras over k.*

b) *Suppose that $(C', b', S', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ is an object of $\mathcal{C}_{cq}$ and $f : (C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) \longrightarrow (C', b', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ is a morphism of oriented quantum coalgebras over k. There is a morphism $F : (\mathcal{C}, \boldsymbol{\beta}, \boldsymbol{S}, \boldsymbol{T}_{\mathsf{d}}, \boldsymbol{T}_{\mathsf{u}}) \longrightarrow (C', b', S', T'_{\mathsf{d}}, T'_{\mathsf{u}})$ uniquely determined by $F \circ \imath = f$.*

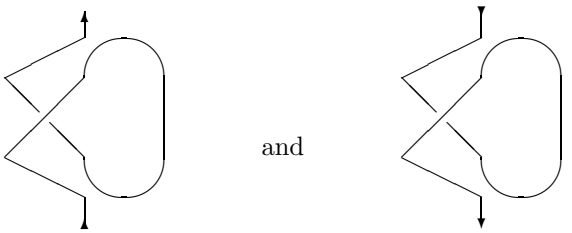
□

7. A Regular Isotopy Invariant of Oriented 1–1 Tangles Which Arises from an Oriented Quantum Coalgebra

In this section we construct a regular isotopy invariant $\mathbf{Inv}_C$ of oriented 1–1 tangle diagrams from an oriented quantum coalgebra C over k in much the same

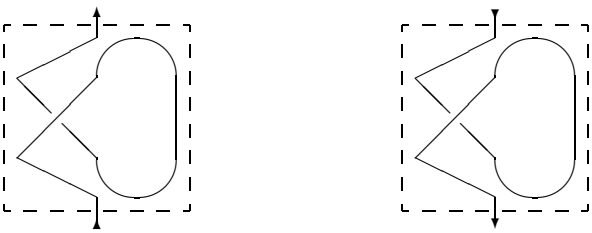
manner that we constructed an invariant of 1–1 tangle diagrams from a quantum coalgebra over k in [**11**, Section 6.1]. The invariant we construct can be considered the coalgebra version of the invariant of oriented 1–1 tangle diagrams described in [**9**, Section 1] and [**8**, Section 3] which arises from an oriented quantum algebra. In Section 7.1 we describe $\mathbf{Inv}_C$ and in Section 7.2 we prove that $\mathbf{Inv}_C$ is a regular isotopy invariant of oriented 1–1 tangle diagrams (and thus determines a regular isotopy invariant of oriented 1–1 tangles).

7.1. Invariants of Oriented 1–1 Tangle Diagrams Arising from Oriented Quantum Coalgebras. We represent oriented 1–1 tangles as diagrams in the plane with respect to the vertical direction. Simple examples of these diagrams are

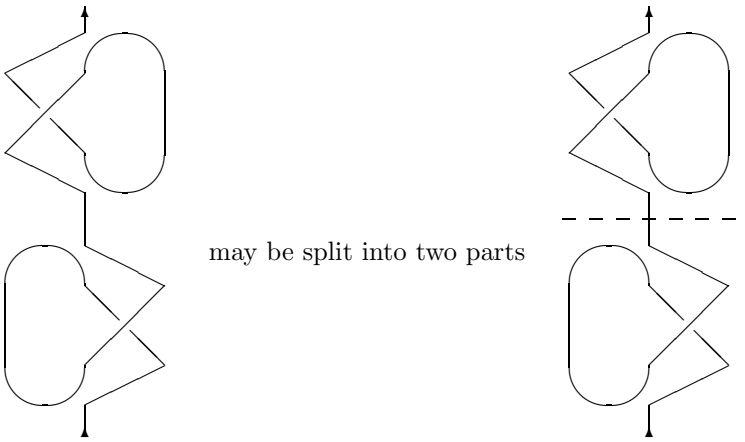


where the arrow heads indicate orientation. We shall refer to the tangle diagrams above as $\mathbf{T}_{\text{curl}}$ and $\mathbf{T}_{\text{curl}}^{op}$ respectively. We let **Tang** denote the set of all oriented 1–1 tangle diagrams. If $\mathbf{T} \in \mathbf{Tang}$ then $\mathbf{T}^{op}$ is the underlying diagram of $\mathbf{T}$ with the opposite orientation.

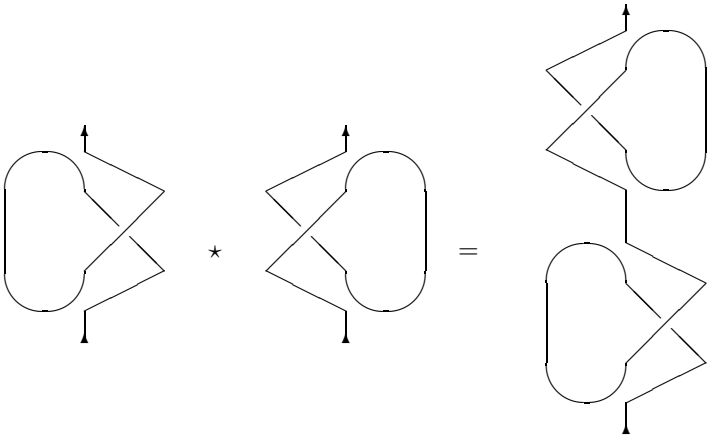
The point on the tangle diagram at which a traversal of the diagram in the direction of the orientation begins is called the *base point of the diagram* and the point at which such a traversal ends is called the *end point of the diagram*. We require 1–1 tangle diagrams to be completely contained in a box except for two protruding line segments as indicated by the two examples below.



When an oriented 1–1 tangle diagram $\mathbf{T}$ can be written as the union of two 1–1 tangle diagrams $\mathbf{T}_1$ and $\mathbf{T}_2$, where the end point of $\mathbf{T}_1$ is the base point of $\mathbf{T}_2$, and the horizontal line passing through this common point otherwise separates $\mathbf{T}_1$ and $\mathbf{T}_2$, then $\mathbf{T}$ is called the *product of* $\mathbf{T}_1$ and $\mathbf{T}_2$ and we write $\mathbf{T} = \mathbf{T}_1 \star \mathbf{T}_2$. For example,



and thus



Multiplication is clearly an associative operation.

Oriented 1–1 tangle diagrams consist of some or all of the following components:

- oriented crossings;

under crossings

over crossings

- oriented local extrema;

local maxima 

local minima 

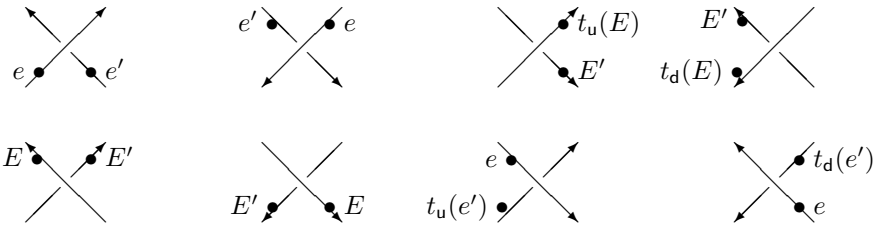
and

- oriented "vertical" lines.

The orientations of adjoining components of the tangle diagram must be compatible.

For an oriented quantum coalgebra $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ over the field k the invariant we describe in this section is a function $\mathbf{Inv}_C : \mathbf{Tang} \longrightarrow C^*$ which is the function $\mathbf{Inv}_A$ of [**9**, Section 1] and [**8**, Section 3] when C is finite-dimensional, strict and $A = C^*$ is the dual quantum algebra. To motivate the definition of $\mathbf{Inv}_C$ we first review how $\mathbf{Inv}_A$ is constructed for oriented quantum algebras A over k. The reader is encouraged to refer to [**9**, Section 1] or [**8**, Section 3] at this point. Much of the discussion which follows parallels [**11**, Section 6.1].

Let $(A, \rho, t_{\mathsf{d}}, t_{\mathsf{u}})$ be an oriented quantum algebra defined over the field k and suppose that $\mathbf{T} \in \mathbf{Tang}$. We decorate each crossing of $\mathbf{T}$ according to the scheme



where we use the shorthand $\rho = e \otimes e'$, $\rho^{-1} = E \otimes E'$ and $(1_A \otimes t)(\rho) = e \otimes t(e')$, $(t \otimes 1_A)(\rho^{-1}) = t(E) \otimes E'$ for $t = t_{\mathsf{d}}, t_{\mathsf{u}}$. In practice we let $e \otimes e'$, $f \otimes f'$, $g \otimes g' \ldots$ denote copies of ρ and $E \otimes E'$, $F \otimes F'$, $G \otimes G' \ldots$ denote copies of ρ^{-1}.

Think of the oriented tangle as a rigid wire and think of the decorations as labeled beads which slide freely around the wire. Starting at the base point of the tangle diagram, traverse the diagram pushing the labeled beads along the wire so that the end result is a juxtaposition of labeled beads at the end point of the diagram. As a labeled bead passes through a local extrema its label is altered according to the following rules:

and

for clockwise motion;

and

for counterclockwise motion. We refer to the oriented local extrema

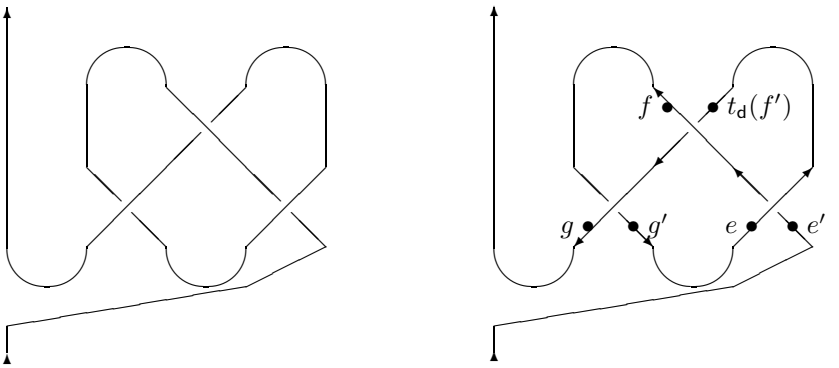
as having type (u_-), (u_+), (d_+) and (d_-) respectively. Reading the juxtaposed labeled beads in the direction of orientation results in a formal word $\mathbf{W}_A(\mathbf{T})$.

Now to define $\mathbf{W}_A(\mathbf{T})$ more formally. If $\mathbf{T}$ has no crossings then $\mathbf{W}_A(\mathbf{T}) = 1$. Suppose that $\mathbf{T}$ has $n \geq 1$ crossings. Traverse $\mathbf{T}$ in the direction of orientation and label the crossing lines $1, 2, \ldots, 2n$ in the order in which they are encountered. For $1 \leq \imath \leq 2n$ let $u_{\mathsf{d}}(\imath)$ be the number of local extrema of type (d_+) minus the number of type (d_-) encountered on the portion of the traversal from line $\imath$ to the end of the traversal of $\mathbf{T}$. We define $u_{\mathsf{u}}(\imath)$ in the same way where (u_+) and (u_-) replace (d_+) and (d_-) respectively. Then

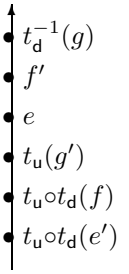
$$\mathbf{W}_A(\mathbf{T}) = t_{\mathsf{d}}^{u_{\mathsf{d}}(1)} \circ t_{\mathsf{u}}^{u_{\mathsf{u}}(1)}(x_1) \cdots t_{\mathsf{d}}^{u_{\mathsf{d}}(2n)} \circ t_{\mathsf{u}}^{u_{\mathsf{u}}(2n)}(x_{2n}), \tag{8}$$

where $x_\imath$ is the decoration on the crossing line $\imath$. Replacing the formal representations of ρ and ρ^{-1} in $\mathbf{W}_A(\mathbf{T})$ by ρ and ρ^{-1} respectively we obtain an element $\mathbf{Inv}_A(\mathbf{T}) \in A$.

For example, consider the oriented 1–1 tangle diagram $\mathbf{T}_{\text{trefoil}}$ depicted below on the left.



Traversal of the 1–1 tangle diagram $\mathbf{T}_{\text{trefoil}}$ results in the juxtaposition of labeled beads



Thus

$$\mathbf{W}_A(\mathbf{T}_{\text{trefoil}}) = \left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(e')\right)\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(f)\right)\left(t_{\mathsf{u}}(g')\right)ef'\left(t_{\mathsf{d}}^{-1}(g)\right)$$

from which we obtain after substitution

$$\mathbf{Inv}_A(\mathbf{T}_{\text{trefoil}}) = \sum_{\imath,\jmath,\ell=1}^{r}\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\imath)\right)\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(a_\jmath)\right)\left(t_{\mathsf{u}}(b_\ell)\right)a_\imath b_\jmath\left(t_{\mathsf{d}}^{-1}(a_\ell)\right),$$

where $\rho = \sum_{\imath=1}^{r} a_\imath\otimes b_\imath \in A\otimes A$. Generally, the formal word $\mathbf{W}_A(\mathbf{T})$ can be viewed as merely a device which encodes instructions for defining an element of A. Since $\rho = (t\otimes t)(\rho)$ and $\rho^{-1} = (t\otimes t)(\rho^{-1})$, or symbolically $e\otimes e' = t(e)\otimes t(e')$ and $E\otimes E' = t(E)\otimes t(E')$ for $t = t_{\mathsf{d}}, t_{\mathsf{u}}$, we may introduce the rules

$$\mathbf{W}_A(\mathbf{T}) = \cdots t^p(x)\cdots t^q(y)\cdots = \cdots t^{p+\ell}(x)\cdots t^{q+\ell}(y)\cdots$$

for all integers ℓ, where $x\otimes y$ or $y\otimes x$ represents either ρ or ρ^{-1}. Thus we may rewrite

$$\mathbf{Inv}_A(\mathbf{T}_{\text{trefoil}}) = \sum_{\imath,\jmath,\ell=1}^{r}\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\imath)\right)\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(a_\jmath)\right)\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\ell)\right)a_\imath b_\jmath a_\ell.$$

As a small exercise the reader is left to show that

$$\begin{aligned}
&\mathbf{Inv}_A(\mathbf{T}^{op}_{\text{trefoil}})\\
&\quad= \sum_{\ell,\jmath,\imath=1}^{r}\left(t_{\mathsf{u}}^{-2}\circ t_{\mathsf{d}}^{-1}(a_\ell)\right)\left(t_{\mathsf{u}}^{-1}\circ t_{\mathsf{d}}^{-1}(b_\jmath)\right)\left(t_{\mathsf{u}}^{-1}\circ t_{\mathsf{d}}^{-1}(a_\imath)\right)\left(t_{\mathsf{u}}^{-1}(b_\ell)\right)a_\jmath b_\imath\\
&\quad= \sum_{\ell,\jmath,\imath=1}^{r} a_\ell b_\jmath a_\imath\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\ell)\right)\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(a_\jmath)\right)\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\imath)\right),
\end{aligned}$$

and also that

$$\mathbf{Inv}_A(\mathbf{T}_{\text{curl}}) = \sum_{\imath=1}^{r} a_\imath\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\imath)\right), \quad \mathbf{Inv}_A(\mathbf{T}^{op}_{\text{curl}}) = \sum_{\imath=1}^{r}\left(t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\imath)\right)a_\imath.$$

Assume that A is a finite-dimensional and let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) = (A^*, b_\rho, t_{\mathsf{d}}^*, t_{\mathsf{u}}^*)$ be the dual (strict) oriented quantum coalgebra. For all $\mathbf{T}\in\mathbf{Tang}$ we regard $\mathbf{Inv}_A(\mathbf{T})\in A = A^{**} = C^*$ as a functional on C. Here we think of A as A^{**} under the identification $a(a^*) = a^*(a)$ for all $a\in A$ and $a^*\in A^*$. We set $\mathbf{Inv}_C = \mathbf{Inv}_A$. Thus for $\mathbf{T}\in\mathbf{Tang}$ the functional $\mathbf{Inv}_C(\mathbf{T})\in A = C^*$ is evaluated on $c\in C$ as follows. Use (8) to make the formal calculation

$$\mathbf{W}_A(\mathbf{T})(c) = c(\mathbf{W}_A(\mathbf{T})) = c_{(1)}(t_{\mathsf{d}}^{u_{\mathsf{d}}(1)}\circ t_{\mathsf{u}}^{u_{\mathsf{u}}(1)}(x_1))\cdots c_{(2n)}(t_{\mathsf{d}}^{u_{\mathsf{d}}(2n)}\circ t_{\mathsf{u}}^{u_{\mathsf{u}}(2n)}(x_{2n}))$$

and replace the formal copies of ρ and ρ^{-1} by their actual values to obtain a scalar $\mathbf{Inv}_C(\mathbf{T})(c)$.

We will evaluate $\mathbf{Inv}_C(\mathbf{T}_{\text{trefoil}})(c)$ to illustrate this procedure. Recall that $b(c,d) = (c\otimes d)(\rho) = \sum_{\imath=1}^{r} c(a_\imath)d(b_\imath)$ for all $c, d\in C$. Thus we calculate, omitting

the summation symbol,

$$\begin{aligned}
&\mathbf{Inv}_C(\mathbf{T}_{\text{trefoil}})(c)\\
&\quad= \quad c\big(\ \big(\ t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\imath)\big)\ \big(\ t_{\mathsf{u}}\circ t_{\mathsf{d}}(a_\jmath)\big)\ \big(\ t_{\mathsf{u}}(b_\ell)\big)\ a_\imath b_\jmath\ \big(\ t_{\mathsf{d}}^{-1}(a_\ell)\big)\big)\\
&\quad= \quad c_{(1)}\ \big(\ t_{\mathsf{u}}\circ t_{\mathsf{d}}(b_\imath)\big)\ c_{(2)}\ \big(\ t_{\mathsf{u}}\circ t_{\mathsf{d}}(a_\jmath)\big)\ c_{(3)}\ \big(\ t_{\mathsf{u}}(b_\ell)\big)\ c_{(4)}(a_\imath)c_{(5)}(b_\jmath)c_{(6)}\ \big(\ t_{\mathsf{d}}^{-1}(a_\ell)\big)\\
&=\big(\ T_{\mathsf{u}}\circ T_{\mathsf{d}}(c_{(1)})(b_\imath)\big)\ \big(\ T_{\mathsf{u}}\circ T_{\mathsf{d}}(c_{(2)})(a_\jmath)\big)\ \big(\ T_{\mathsf{u}}(c_{(3)})(b_\ell)\big)\ c_{(4)}(a_\imath)c_{(5)}(b_\jmath)\ \big(\ T_{\mathsf{d}}^{-1}(c_{(6)})(a_\ell)\big)\\
&\quad= \quad b(c_{(4)}, T_{\mathsf{d}}\circ T_{\mathsf{u}}(c_{(1)}))b(T_{\mathsf{d}}\circ T_{\mathsf{u}}(c_{(2)}), c_{(5)})b(T_d^{-1}(c_{(6)}), T_{\mathsf{u}}(c_{(3)}))
\end{aligned}$$

and thus

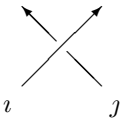
$$\mathbf{Inv}_C(\mathbf{T}_{\text{trefoil}})(c) = b(c_{(4)}, T_{\mathsf{d}}\circ T_{\mathsf{u}}(c_{(1)}))b(T_{\mathsf{d}}\circ T_{\mathsf{u}}(c_{(2)}), c_{(5)})b(T_d^{-1}(c_{(6)}), T_{\mathsf{u}}(c_{(3)}))$$

for all $c \in C$.

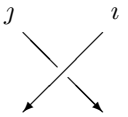
Now suppose that $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is any oriented quantum coalgebra over k. We shall define $\mathbf{Inv}_C$ in a way which agrees with our definition when C is the dual of a finite-dimensional oriented quantum algebra over k.

Let $\mathbf{T} \in \mathbf{Tang}$. If $\mathbf{T}$ has no crossings set $\mathbf{Inv}_C(\mathbf{T}) = \epsilon$. Suppose that $\mathbf{T}$ has $n \geq 1$ crossings. Starting at the base point of the tangle diagram $\mathbf{T}$, traverse $\mathbf{T}$ labeling the crossing lines of the diagram $1, \dots, 2n$ in the order encountered. For $1 \leq \imath \leq 2n$ let $u_{\mathsf{d}}(\imath)$ and $u_{\mathsf{u}}(\imath)$ be as defined earlier in this section.

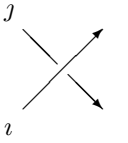
Let χ be a crossing and suppose that its over crossing and under crossing lines are labeled $\imath$ and $\jmath$ respectively. For $c \in C$ the scalar $\mathbf{Inv}_C(\mathbf{T})(c)$ is the sum of products, where each crossing contributes a factor according to:



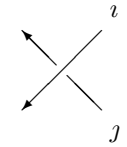
$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)}))\cdots$$



$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)}))\cdots$$

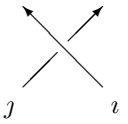


$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)+1}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)}))\cdots$$

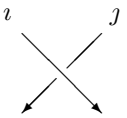


$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)+1}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)}))\cdots$$

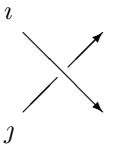
for under crossings;



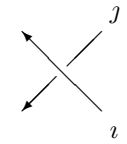
$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})) \cdots$$



$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})) \cdots$$



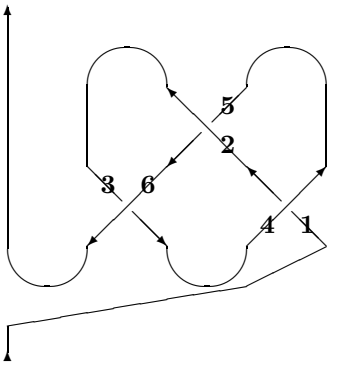
$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)+1}(c_{(\jmath)})) \cdots$$



$$\mathbf{Inv}_C(\mathbf{T})(c) = \cdots b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)+1} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})) \cdots$$

for over crossings. In the next section we will show that $\mathbf{Inv}_C$ determines a regular isotopy invariant of 1–1 tangle diagrams.

Let us reconsider the tangle diagram $\mathbf{T}_{\text{Trefoil}}$. Diagram traversal results in the labeling



and thus

$$\mathbf{Inv}_C(\mathbf{T}_{\text{trefoil}})(c) = b(c_{(4)}, T_{\mathsf{d}} \circ T_{\mathsf{u}}(c_{(1)}))b(T_{\mathsf{d}} \circ T_{\mathsf{u}}(c_{(2)}), c_{(5)})b(T_d^{-1}(c_{(6)}), T_{\mathsf{u}}(c_{(3)}))$$

for all $c \in C$ by the algorithm described above which agrees with our previous calculation. Observe that

$$\mathbf{Inv}_C(\mathbf{T}_{\text{curl}})(c) = b(T_{\mathsf{d}} \circ T_{\mathsf{u}}(c_1), c_{(2)}) \quad \text{and} \quad \mathbf{Inv}_C(\mathbf{T}_{\text{curl}}^{op})(c) = b(T_{\mathsf{d}} \circ T_{\mathsf{u}}(c_2), c_{(1)}).$$

Note that if $\mathbf{T}, \mathbf{T}', \mathbf{T}'' \in \mathbf{Tang}$ and $\mathbf{T}'' = \mathbf{T} \star \mathbf{T}'$ then

$$\mathbf{Inv}_C(\mathbf{T} \star \mathbf{T}') = \mathbf{Inv}_C(\mathbf{T})\mathbf{Inv}_C(\mathbf{T}'),$$

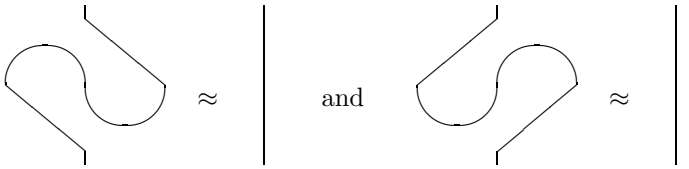
where the righthand side of the equation is the product in the dual algebra C^*.

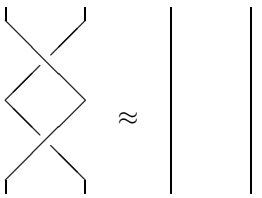
7.2. A Proof That $\mathbf{Inv}_C$ Determines a Regular Isotopy Invariant of Oriented 1–1 Tangles. The sole purpose of this section is to show that the function $\mathbf{Inv}_C$ of Section 7.1 determines a regular isotopy invariant of oriented 1–1 tangles. This follows by:

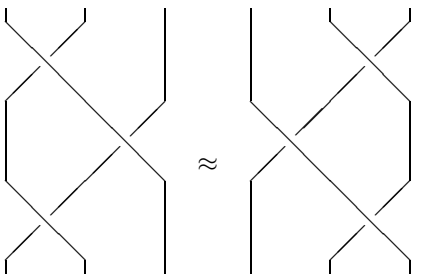
THEOREM 4. *Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ be an oriented quantum coalgebra defined over the field k and suppose that $\mathbf{Inv}_C : \mathbf{Tang} \longrightarrow C^*$ is the function of the previous section. If $\mathbf{T}, \mathbf{T}' \in \mathbf{Tang}$ are regularly isotopic then $\mathbf{Inv}_C(\mathbf{T}) = \mathbf{Inv}_C(\mathbf{T}')$.*

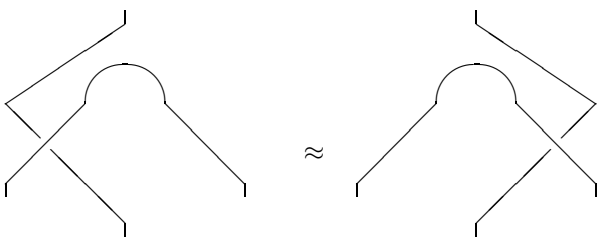
PROOF: The reader will find a discussion of regular isotopy, which we assume as background material, in many references. Here we follow the conventions of [**4**].

The regular isotopy equivalences are

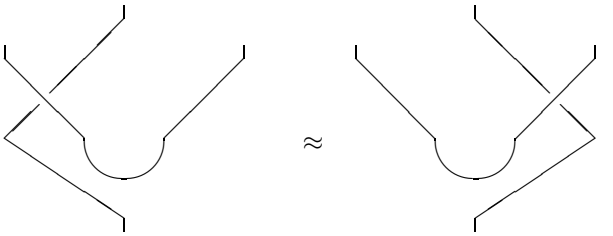
(M.1) 

(M.2) 

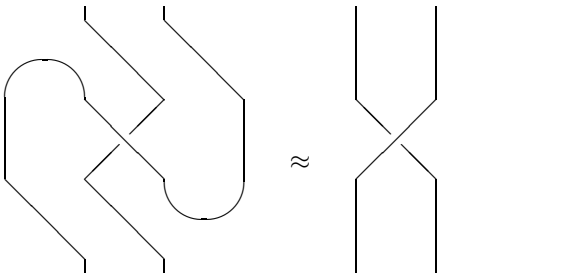
(M.3) 

(M.4) 

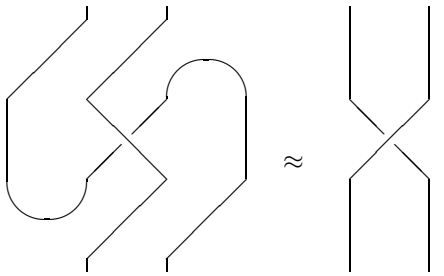
and



and (M.2rev)–(M.4rev), which are (M.2)–(M.4) respectively with over crossings replaced by under crossings and vice versa. The "twist moves"



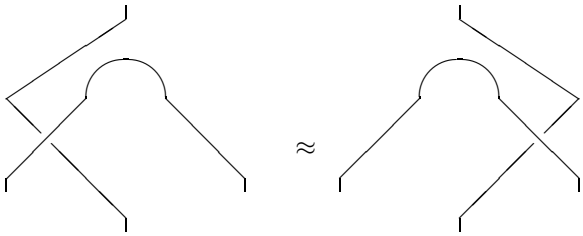
and



are consequences of (M.1), (M.2) and (M.4). These are important in that they allow for crossing types to be changed.

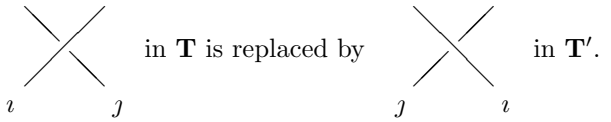
Let $\mathbf{T}, \mathbf{T}' \in \mathbf{Tang}$ and suppose that a part of $\mathbf{T}$ is the figure on the left in one of the equivalences of (M.1)–(M.5) or (M.2rev)–(M.5rev) and that $\mathbf{T}'$ is obtained from $\mathbf{T}$ by replacing the figure on the left with the figure on the right. To prove the theorem we need only show that $\mathbf{Inv}_C(\mathbf{T}) = \mathbf{Inv}_C(\mathbf{T}')$. There are many cases to consider since all possible orientations must be taken into account. We will carefully analyze the typical cases, leaving the remainder for the reader to work out. Let u'_{d} and u'_{u} be the counterparts of u_{d} and u_{u} respectively for $\mathbf{T}'$.

Consider the first equivalence



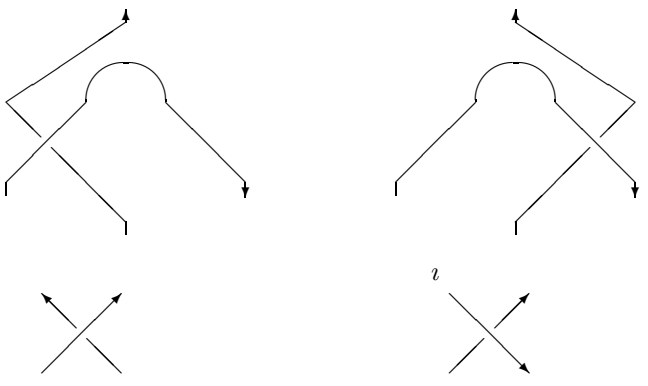
(9)

of (M.4). In this case



There are four possible orientations associated with (9).

Case M.4.1:

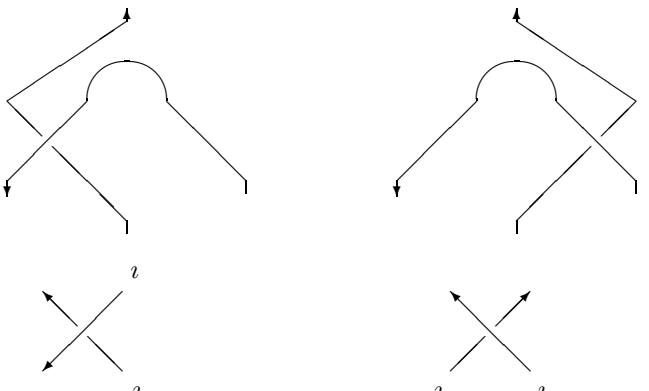


Observe that u'_{d} and u'_{u} agree with u_{d} and u_{u} respectively with the exception $u'_{\mathsf{u}}(\imath) = u_{\mathsf{u}}(\imath) + 1$. Since $T_{\mathsf{d}}, T_{\mathsf{u}}$ commute and (qc.2) holds for b it follows that

$$\begin{aligned} & b(T_{\mathsf{d}}^{u'_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u'_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u'_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u'_{\mathsf{u}}(\jmath)+1}(c_{(\jmath)})) \\ = \; & b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)+1}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)+1}(c_{(\jmath)})) \\ = \; & b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})) \end{aligned}$$

The contributions which the other crossings of $\mathbf{T}$ make to $\mathbf{Inv}_C(\mathbf{T})(c)$ are unaffected by the replacement of the figure on the left in (9) with the right on the right. Therefore $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ in this case.

Case M.4.2:



Observe that u'_{d} and u'_{u} agree with u_{d} and u_{u} respectively with the exception $u'_{\mathsf{d}}(\imath) = u_{\mathsf{d}}(\imath) + 1$.

Since

$$\begin{aligned} & b^{-1}(T_{\mathsf{d}}^{u'_{\mathsf{d}}(\imath)} \circ T_{\mathsf{u}}^{u'_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u'_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u'_{\mathsf{u}}(\jmath)}(c_{(\jmath)})) \\ = \quad & b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)+1} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)} \circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)}) \end{aligned}$$

and the contributions which the other crossings of $\mathbf{T}$ make to $\mathbf{Inv}_C(\mathbf{T})(c)$ are unaffected by the replacement of the figure on the left in (9) with the right on the right, $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ in this case.

The calculations in the other two cases, which are Cases M.4.1 and M.4.2 with orientations reversed, are similar to those in Cases M.4.1 and M.4.2 respectively. Thus $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ when $\mathbf{T}$ is altered according to (9).

By a similar argument it follows that $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ when $\mathbf{T}$ is altered according to the second equivalence of (M.4) and, since (qc.2) holds for b^{-1} also, $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ when $\mathbf{T}$ is altered according to (M.4rev).

It is clear that $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ when $\mathbf{T}$ is altered according to (M.1). The following non-standard notation for the coproduct

$$\begin{aligned} \Delta^{(m-1)}(c) \quad &= \quad c_{(1)} \otimes \cdots \otimes c_{(\ell)} \otimes c_{(\ell+1)} \otimes \cdots \otimes c_{(\ell')} \otimes c_{(\ell'+1)} \cdots \otimes c_{(m)} \\ &= \quad c_{(1)} \otimes \cdots \otimes c_{(\ell)(1)} \otimes c_{(\ell)(2)} \otimes \cdots \otimes c_{(\ell')(1)} \otimes c_{(\ell')(2)} \cdots \otimes c_{(m)} \end{aligned}$$

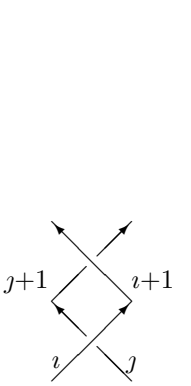
will be very useful in our analysis of (M.2). To emphasize, in the second expression for $\Delta^{(m-1)}$ differs from the first *only* in that the subscripts $(\ell), (\ell{+}1)$ are replaced by $(\ell)(1), (\ell)(2)$ and that $(\ell'), (\ell'{+}1)$ are replaced by $(\ell')(1), (\ell')(2)$. Likewise the non-standard notation

$$\begin{aligned} & \Delta^{(m-1)}(c) \\ & \quad = \quad c_{(1)} \otimes \cdots \otimes c_{(\ell)} \otimes c_{(\ell+1)} \cdots \otimes c_{(\ell')} \otimes c_{(\ell'+1)} \cdots \otimes c_{(\ell'')} \otimes c_{(\ell''+1)} \cdots \otimes c_{(m)} \\ & \quad = \quad c_{(1)} \otimes \cdots \otimes c_{(\ell)(1)} \otimes c_{(\ell)(2)} \cdots \otimes c_{(\ell')(1)} \otimes c_{(\ell')(2)} \cdots \otimes c_{(\ell'')(1)} \otimes c_{(\ell'')(2)} \cdots \otimes c_{(m)} \end{aligned}$$

will be very useful in our analysis of our analysis of (M.3). These manipulations with the subscripts are justified the coassociativity of the coproduct.

We consider (M.2) next. There are four cases to analyze.

Case M.2.1:



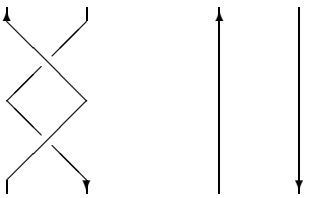
In this case in $\mathbf{T}$ is replaced by in $\mathbf{T}'$. Since b^{-1} is right inverse of b and $T_{\mathsf{d}}, T_{\mathsf{u}}$ are commuting coalgebra automorphisms of C with respect to $\{b, b^{-1}\}$, it follows by part a) of Lemma 1 that the contribution which

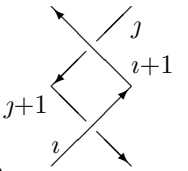
the two crossings above make to the calculation of $\mathbf{Inv}_C(\mathbf{T})(c)$ is

$$\begin{aligned}
& b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)}))\times \\
& \qquad b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath+1)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath+1)})) \\
= \;& b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)(1)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)(1)}))\times \\
& \qquad b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)(2)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)(2)})) \\
= \;& b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)})_{(1)}, T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})_{(1)})\times \\
& \qquad b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)})_{(2)}, T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})_{(2)}) \\
= \;& \epsilon(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}))\epsilon(T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\imath')})) \\
= \;& \epsilon(c_{(\imath)})\epsilon(c_{(\jmath)}) \\
= \;& \epsilon(c_{(\imath)(1)})\epsilon(c_{(\imath)(2)})\epsilon(c_{(\jmath)(1)})\epsilon(c_{(\jmath)(2)}) \\
= \;& \epsilon(c_{(\imath)})\epsilon(c_{(\imath+1)})\epsilon(c_{(\jmath)})\epsilon(c_{(\jmath+1)}).
\end{aligned}$$

Since the contributions which the other crossings of $\mathbf{T}$ make to $\mathbf{Inv}_C(\mathbf{T})(c)$ are unaffected by the replacement of the figure on the left in Case M.2.1 with the right on the right, $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ in this case.

Case M.2.2:



In this case  in $\mathbf{T}$ is replaced by  in $\mathbf{T}'$. Since $T_{\mathsf{d}}, T_{\mathsf{u}}$ are commuting coalgebra automorphisms of C with respect to $\{b, b^{-1}\}$, it follows by part b) of Lemma 1 and the second equation of (qc.1) that the contribution

which the two crossings above make to the calculation of $\mathbf{Inv}_C(\mathbf{T})(c)$ is

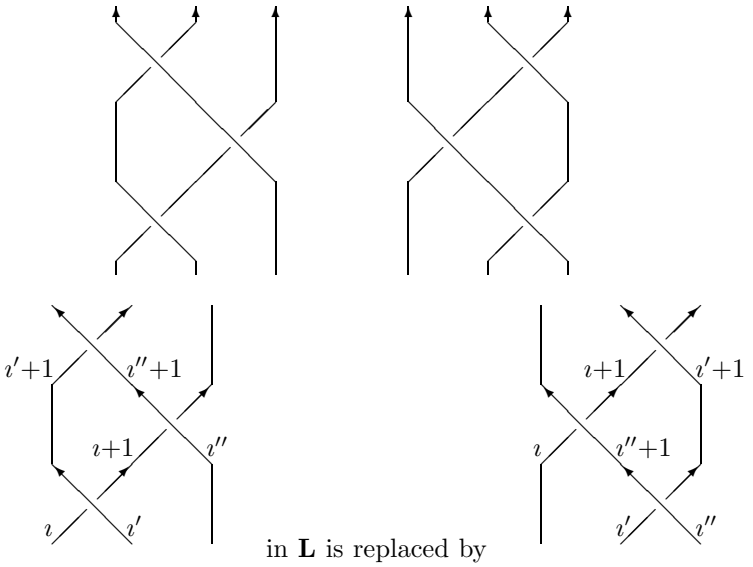
$$\begin{aligned}
& b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)+1}(c_{(\imath)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)}))\times \\
&\qquad b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath+1)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)+1}(c_{(\jmath)})) \\
=\ & b^{-1}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)+1}(c_{(\imath)(1)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)(2)}))\times \\
&\qquad b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)(2)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)+1}(c_{(\jmath)(1)})) \\
=\ & b^{-1}(T_{\mathsf{u}}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)})_{(1)}), T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})_{(2)})\times \\
&\qquad b(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)})_{(2)}, T^{\mathsf{u}}(T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\jmath)})_{(1)}))) \\
=\ & \epsilon(T^{u(\imath)}(c_{(\imath)}))\epsilon(T^{u(\imath')}(c_{(\imath')})) \\
=\ & \epsilon(T_{\mathsf{d}}^{u_{\mathsf{d}}(\imath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\imath)}(c_{(\imath)}))\epsilon(T_{\mathsf{d}}^{u_{\mathsf{d}}(\jmath)}\circ T_{\mathsf{u}}^{u_{\mathsf{u}}(\jmath)}(c_{(\imath')})) \\
=\ & \epsilon(c_{(\imath)})\epsilon(c_{(\jmath)}) \\
=\ & \epsilon(c_{(\imath)(1)})\epsilon(c_{(\imath)(2)})\epsilon(c_{(\jmath)(1)})\epsilon(c_{(\jmath)(2)}) \\
=\ & \epsilon(c_{(\imath)})\epsilon(c_{(\imath+1)})\epsilon(c_{(\jmath)})\epsilon(c_{(\jmath+1)}).
\end{aligned}$$

Since the contributions which the other crossings of $\mathbf{T}$ make to $\mathbf{Inv}_C(\mathbf{T})(c)$ are unaffected by the replacement of the figure on the left in Case M.2.1 with the right on the right, $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ in this case.

Using the fact that b^{-1} is a left inverse for b the argument for Cases M.2.1 is easily modified to show that $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ in Case M.2.3, which is Case M.2.1 with orientations reversed. Using the first equation of (qc.1) the argument for Cases M.2.2 is easily modified to show that $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ in Case M.2.4, which is Case M.2.2 with orientations reversed.

It remains to analyze (M.3). We consider the possible orientations of the lines of the figures described in (M.3), reading left to right.

Case M.3.1



In this case in $\mathbf{L}$ is replaced by in $\mathbf{L}'$. Since $u(\imath+1) = u(\imath)$, $u(\imath'+1) = u(\imath')$ and $u(\imath''+1) = u(\imath'')$, the contribution which

the figure on the left above makes to the calculation of $\mathbf{Inv}_C(\mathbf{T})(c)$ is

$$b^{-1}(T^{u(\imath'')}(c_{(2)}), T^{u(\imath')}(d_{(2)}))b^{-1}(T^{u(\imath'')}(c_{(1)}), T^{u(\imath)}(e_{(2)}))b^{-1}(T^{u(\imath')}(d_{(1)}), T^{u(\imath)}(e_{(1)}))$$

and the contribution which the figure on the right above makes to the calculation of $\mathbf{Inv}_C(\mathbf{T}')(c)$ is

$$b^{-1}(T^{u(\imath'')}(c_{(1)}), T^{u(\imath')}(d_{(1)}))b^{-1}(T^{u(\imath'')}c_{(2)}, T^{u(\imath)})(e_{(1)}))b^{-1}(T^{u(\imath')}d_{(2)}, T^{u(\imath)})(e_{(2)}))$$

where $c = c_{(\imath'')}$, $d = c_{(\imath'')}$, and $e = c_{(\imath)}$. By part a) of Lemma 1 the two contributions are the same if

$$\begin{aligned} & b^{-1}(c_{(2)}, T^v(d_{(2)}))b^{-1}(c_{(1)}, e_{(1)})b^{-1}(T^v(d_{(1)}), e_{(2)}) \\ = \quad & b^{-1}(c_{(1)}, T^v(d_{(1)}))b^{-1}(c_{(2)}, e_{(1)})b^{-1}(T^v(d_{(2)}), e_{(2)}) \end{aligned}$$

for all $c, d, e \in C$. Since b^{-1} satisfies (qc.2), using part a) of Lemma 1 again we see that this last equation holds if and only if

$$\begin{aligned} & b^{-1}(T^{-v}(c_{(2)}), d_{(2)})b^{-1}(T^{-v}(c_{(1)}), T^{-v}(e_{(1)}))b^{-1}(d_{(1)}, T^{-v}(e_{(2)})) \\ = \quad & b^{-1}(T^{-v}(c_{(1)}), d_{(1)})b^{-1}(T^{-v}(c_{(2)}), T^{-v}(e_{(1)}))b^{-1}(T^v(d_{(2)}), e_{(2)}) \end{aligned}$$

holds for all $c, d, e \in C$ if and only if

$$\begin{aligned} & b^{-1}(T^{-v}(c)_{(2)}, d_{(2)})b^{-1}(T^{-v}(c)_{(1)}, T^{-v}(e)_{(1)})b^{-1}(d_{(1)}, T^{-v}(e)_{(2)}) \\ = \quad & b^{-1}(T^{-v}(c)_{(1)}, d_{(1)})b^{-1}(T^{-v}(c)_{(2)}, T^{-v}(e)_{(2)})b^{-1}(d_{(2)}, T^{-v}(e)_{(1)})) \end{aligned}$$

holds for all $c, d, e \in C$ which in turn holds if and only if

$$\begin{aligned} & b^{-1}(c_{(2)}, d_{(2)})b^{-1}(c_{(1)}, e_{(1)})b^{-1}(d_{(1)}, e_{(2)}) \\ = \quad & b^{-1}(c_{(1)}, d_{(1)})b^{-1}(c_{(2)}, e_{(1)})b^{-1}(d_{(2)}, e_{(2)}) \end{aligned}$$

holds for all $c, d, e \in C$. The last equation is (qc.3) for b^{-1} which holds since (qc.3) holds for b. Thus the two contributions are the same. Since the contributions which the other crossings of $\mathbf{T}$ make to $\mathbf{Inv}_C(\mathbf{T})(c)$ are unaffected by the replacement of the figure on the left in Case M.3.1 with the right on the right, $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ in Case M.3.1.

Using similar arguments one can show that $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ for all $c \in C$ in Case M.3.2 (up up down) if

$$\begin{aligned} & b^{-1}(c_{(2)}, d_{(2)})b(c_{(1)}, e_{(1)})b(d_{(1)}, e_{(2)}) \\ = \quad & b^{-1}(c_{(1)}, d_{(1)})b(c_{(2)}, e_{(2)})b(d_{(2)}, e_{(1)}) \end{aligned} \tag{10}$$

for all $c, d, e \in C$, in Case M.3.3 (up down up) if

$$\begin{aligned} & b(c_{(2)}, d_{(1)})b^{-1}(c_{(1)}, e_{(2)})b(d_{(2)}, T^2(e_{(1)})) \\ = \quad & b(c_{(1)}, d_{(2)})b^{-1}(c_{(2)}, e_{(1)})b(d_{(1)}, T^2(e_{(2)})) \end{aligned} \tag{11}$$

for all $c, d, e \in C$, and in Case M.3.4 (up down down) if

$$\begin{aligned} & b(c_{(2)}, d_{(1)})b(c_{(1)}, e_{(1)})b^{-1}(d_{(2)}, e_{(2)}) \\ = \quad & b(c_{(1)}, d_{(2)})b(c_{(2)}, e_{(2)})b^{-1}(d_{(1)}, e_{(1)}) \end{aligned} \tag{12}$$

for all $c, d, e \in C$. Cases M.2.5–M.3.8, which are Cases M.3.1–M.3.4 with orientations reversed, reduce to Cases M.3.1–M.3.4. Cases M.3rev.1–M.3rev.8 are Cases M.3.1–M.3.8 for the oriented quantum coalgebra (C, b^{-1}, T^{-1}). Thus to complete the proof of the theorem we need only establish (10)–(12).

To establish (10) we define linear maps $\ell, r, u : C\otimes C\otimes C \longrightarrow k$ by

$$\ell(c\otimes d\otimes e) = b^{-1}(c_{(2)}, d_{(2)})b(c_{(1)}, e_{(1)})b(d_{(1)}, e_{(2)}),$$
$$r(c\otimes d\otimes e) = b^{-1}(c_{(1)}, d_{(1)})b(c_{(2)}, e_{(2)})b(d_{(2)}, e_{(1)})$$

and

$$u(c\otimes d\otimes e) = b(c, d)\epsilon(e)$$

for all $c, d, e \in C$. Since u is invertible in the dual algebra $(C\otimes C\otimes C)^*$ and $u\ell u = uru$, we conclude that $\ell = r$, which is to say that (10) holds.

To establish (12) we define linear maps $\ell, r, u : C\otimes C\otimes C \longrightarrow k$ by

$$\ell(c\otimes d\otimes e) = b(c_{(2)}, d_{(1)})b(c_{(1)}, e_{(1)})b^{-1}(d_{(2)}, e_{(2)}),$$
$$r(c\otimes d\otimes e) = b(c_{(1)}, d_{(1)})b(c_{(2)}, e_{(2)})b^{-1}(d_{(1)}, e_{(1)})$$

and

$$u(c\otimes d\otimes e) = \epsilon(e)b(d, e)$$

for all $c, d, e \in C$. Again, u is invertible in the dual algebra $(C\otimes C\otimes C)^*$ and again $u\ell u = uru$. Thus $\ell = r$, or equivalently (10) holds.

Equation (11) is perhaps the most interesting of (10)–(12). Since T^{-1} is a coalgebra automorphism of C with respect to $\{b, b^{-1}\}$ by part a) of Lemma 1, the equations of (qc.1) can be reformulated

$$b(c_{(1)}, T^2(d_{(2)}))b^{-1}(c_{(2)}, d_{(1)}) = \epsilon(c)\epsilon(d)$$

and

$$b^{-1}(c_{(1)}, d_{(2)})b(c_{(2)}, T^2(d_{(1)})) = \epsilon(c)\epsilon(d)$$

for all $c.d \in C$. Thus the right hand side of the equation of (11)

$$\begin{aligned}
&b(c_{(1)}, d_{(2)})b^{-1}(c_{(2)}, e_{(1)})b(d_{(1)}, T^2(e_{(2)}))\\
&\quad= b^{-1}(c_{(1)}, e_{(4)})b(c_{(3)}, d_{(2)})b^{-1}(c_{(4)}, e_{(1)})b(d_{(1)}, T^2(e_{(2)})b(c_{(2)}, T^2(e_{(3)})))\\
&\quad= b^{-1}(c_{(1)}, e_{(4)})b(c_{(2)}, d_{(1)})b^{-1}(c_{(4)}, e_{(1)})b(d_{(2)}, T^2(e_{(3)})b(c_{(3)}, T^2(e_{(2)})))\\
&\quad= b^{-1}(c_{(1)}, e_{(2)})b(c_{(2)}, d_{(1)})b(d_{(2)}, T^2(e_{(1)}))\\
&\quad= b(c_{(2)}, d_{(1)})b^{-1}(c_{(1)}, e_{(2)})b(d_{(2)}, T^2(e_{(1)}))
\end{aligned}$$

is equal to the left hand side. We have established (11) which completes the proof of the theorem. □

Apropos of the proof of Theorem 4, observe that (10) and (12) reduce to the finite-dimensional case since C is the sum of its finite-dimensional subcoalgebras. For suppose that C is finite-dimensional, $b : C\otimes C \longrightarrow k$ is a bilinear form which is invertible and satisfies (qc.3). Let $R \in C^*\otimes C^*$ be defined by $b(c, d) = R(c\otimes d)$ for all $c, d \in C$. Then R is invertible and $R_{1\,2}R_{1\,3}R_{2\,3} = R_{2\,3}R_{1\,3}R_{1\,2}$. Equations (10) and (12) translate to $R^{-1}_{1\,2}R_{2\,3}R_{1\,3} = R_{1\,3}R_{2\,3}R^{-1}_{1\,2}$ and $R^{-1}_{2\,3}R_{1\,2}R_{1\,3} = R_{1\,3}R_{1\,2}R^{-1}_{2\,3}$ respectively which are consequences of the preceding equation. Also, once $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ for all $c \in C$ is established in the cases for (M.2), (M.4) and in Case M.3.1, necessarily $\mathbf{Inv}_C(\mathbf{T})(c) = \mathbf{Inv}_C(\mathbf{T}')(c)$ for all $c \in C$ in Case M.4.3 for topological reasons.

To calculate the invariant $\mathbf{Inv}_C$ we need only consider standard oriented quantum coalgebras.

THEOREM 5. *Let $(C, b, T_{\mathtt{d}}, T_{\mathtt{u}})$ be an oriented quantum coalgebra over the field k. Then $\mathbf{Inv}(C, b, T_{\mathtt{d}}, T_{\mathtt{u}})(\mathbf{T}) = \mathbf{Inv}_{(C,b,1_C,T_{\mathtt{d}}\circ T_{\mathtt{u}})}(\mathbf{T})$ for all $\mathbf{T} \in \mathbf{Tang}$.*

PROOF: We may assume $\mathbf{T}$ has a crossing and that all of of its crossings are oriented upward. The result now follows as $u_{\mathsf{u}}(\imath) = u_{\mathsf{d}}(\imath)$ for all lines $\imath$ of $\mathbf{T}$. See the discussion preceding [**8**, Proposition 3]. □

The invariants $\mathbf{Inv}_C$ and $\mathbf{Inv}_{C^{cop}}$ have a very natural relationship.

LEMMA 3. *Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ be an oriented quantum coalgebra over k. Then $\mathbf{Inv}_C(\mathbf{T}^{op}) = \mathbf{Inv}_{C^{cop}}(\mathbf{T})$ for all $\mathbf{T} \in \mathbf{Tang}$.*

PROOF: We may assume that $\mathbf{T}$ has $n \geq 1$ crossings. A crossing line of $\mathbf{T}$ which has label $\imath$ in $\mathbf{T}^{op}$ has label $n + \imath - 1$ in $\mathbf{T}$. Let s be the sum of the local extrema of $\mathbf{T}$ which are oriented counter clockwise minus the number oriented clockwise. Then $s = u(n + \imath - 1) - u^{op}(\imath)$, or equivalently $u^{op}(\imath) = u(n + \imath - 1) - s$, for all $1 \leq \imath \leq n$. Thus

$$\begin{aligned}
\mathbf{Inv}_C(\mathbf{T}^{op})(c) &= \dots b^r(T^{u^{op}}(c_{(\imath)}), T^{u^{op}}(c_{(\jmath)})) \dots \\
&= \dots b^r(T^{u(n+\imath-1)-s}(c_{(\imath)}), T^{u(n+\jmath-1)-s}(c_{(\jmath)})) \dots \\
&= \dots b^r(T^{u(n+\imath-1)}(c_{(\imath)}), T^{u(n+\jmath-1)}(c_{(\jmath)})) \dots \\
&= \mathbf{f}_{C^{cop}}(\mathbf{T})(c)
\end{aligned}$$

for all $c \in C$, where $r = \pm 1$. □

8. Oriented 1–1 Tangle Invariants Arising from Cocommutative Oriented Quantum Coalgebras

Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ be an oriented quantum coalgebra over k and suppose that C is cocommutative. To compute $\mathbf{Inv}_C$ we may assume that $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}}) = (C, b, 1_C, T)$ is standard by Theorem 5. Since C is cocommutative it follows by (qc.1) that b and the bilinear form $b' : C \times C \longrightarrow k$ defined by $b'(c, d) = b(c, T(d))$ for all $c, d \in C$ are both inverses for b^{-1}. Therefore $b' = b$, and using (qc.2) we deduce

$$b(c, T(d)) = b(c, d) = b(T(c), d) \tag{13}$$

for all $c, d \in C$. Since T is a coalgebra automorphism of C with respect to $\{b, b^{-1}\}$ it follows by (13) that (13) holds for b^{-1} and T as well; therefore

$$b^r(T^u(c), T^v(d)) = b(c, d) \tag{14}$$

for all integers u, v and $c, d \in C$, where $r = \pm 1$.

Suppose that $\mathbf{T} \in \mathbf{Tang}$ is an oriented 1–1 tangle diagram with $n \geq 1$ crossings. Let $c \in C$. Since C is cocommutative $\Delta^{(2n-1)}(c) = c_{(\imath_1)} \otimes \dots \otimes c_{(\imath_{2n})}$, where $\imath_1, \dots, \imath_{2n}$ is any arrangement of $1, \dots, 2n$; see [**11**, Section 7.4] for example. This last equation and (14) show that any crossing χ of $\mathbf{T}$ with crossing lines labeled $\imath$ and $\jmath$ contributes the factor $b^{\operatorname{sign}\chi}(c_{(\imath)}, c_{(\jmath)})$ to the formulation of $\mathbf{Inv}_C(\mathbf{T})(c)$.

We follow [**4**] in our convention for the sign of an oriented crossing. The sign of an oriented crossing is 1 if as the under crossing line is traversed in the direction of orientation the direction of the over crossing line is to the right, otherwise the sign of the crossing is -1. The writhe of an oriented 1–1 tangle diagram, denoted by $\operatorname{writhe}\mathbf{T}$, is 0 if the tangle has no crossings; otherwise the writhe is defined to be the sum of the signs of the crossings.

Now let $\chi_1, \ldots, \chi_n$ be the crossings of $\mathbf{T}$. Using the cocommutativity of C again we may thus write

$$\begin{aligned}
\mathbf{Inv}_C(\mathbf{T})(c) &= b^{\operatorname{sign}\chi_1}(c_{(1)(1)}, c_{(2)(1)}) \cdots b^{\operatorname{sign}\chi_n}(c_{(1)(n)}, c_{(2)(n)}) \\
&= b_{(\ell)}^{\operatorname{sign}\chi_1}(c_{(1)(1)})(c_{(2)(1)}) \cdots b_{(\ell)}^{\operatorname{sign}\chi_n}(c_{(1)(n)})(c_{(2)(n)}) \\
&= \left(b_{(\ell)}^{\operatorname{sign}\chi_1}(c_{(1)(1)}) \cdots b_{(\ell)}^{\operatorname{sign}\chi_n}(c_{(1)(n)})\right)(c_{(2)}) \\
&= b_{(\ell)}^{\operatorname{sign}\chi_1 + \cdots + \operatorname{sign}\chi_n}(c_{(1)})(c_{(2)}) \\
&= b_{(\ell)}^{\operatorname{writhe}\mathbf{T}}(c_{(1)})(c_{(2)}) \\
&= b^{\operatorname{writhe}\mathbf{T}}(c_{(1)}, c_{(2)}).
\end{aligned}$$

With the convention $b^0(c,d) = \epsilon(c)\epsilon(d)$ for all $c, d \in C$, we conclude that

$$\mathbf{Inv}_C(\mathbf{T})(c) = b^{\operatorname{writhe}\mathbf{T}}(c_{(1)}, c_{(2)}) \tag{15}$$

for all $\mathbf{T} \in \mathbf{Tang}$ and $c \in C$. Thus the regular isotopy invariant writhe of oriented 1–1 tangle diagrams dominates $\mathbf{Inv}_C$, meaning that whenever $\mathbf{T}, \mathbf{T}' \in \mathbf{Tang}$ satisfy $\operatorname{writhe}\mathbf{T} = \operatorname{writhe}\mathbf{T}'$ then $\mathbf{Inv}_C(\mathbf{T}) = \mathbf{Inv}_C(\mathbf{T}')$.

9. Regular Isotopy Invariants of Oriented Knots and Links Which Arise from a Twist Oriented Quantum Coalgebra

Throughout this section $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}}, G)$ is a twist oriented quantum coalgebra over k; that is $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is a strict oriented quantum coalgebra over k and $G \in C^*$ in an invertible element which satisfies $T_{\mathsf{d}}^*(G) = T_{\mathsf{u}}^*(G) = G$ and $T_{\mathsf{d}} \circ T_{\mathsf{u}}(c) = G^{-1} \rightharpoonup c \leftharpoonup G$ for all $c \in C$. The notion of twist quantum coalgebra is introduced in [**7**, Section 4]. Note that $(C^{cop}, b, T_{\mathsf{d}}, T_{\mathsf{u}}, G^{-1})$ is a twist oriented quantum coalgebra as well.

We represent oriented knots and links as diagrams in the plane with respect to the vertical direction. Let $\mathcal{K}$ be the set of oriented knot diagrams and $\mathcal{L}$ be the set of oriented link diagrams with respect to the vertical direction. We will show T-invariant cocommutative elements $\mathsf{c} \in C$ give rise to scalar valued functions $\mathbf{f}_{C,\mathsf{c}} : \mathcal{L} \longrightarrow k$ which are constant on the regular isotopy classes of oriented link diagrams (and thus $\mathbf{f}_{C,\mathsf{c}}$ defines a regular isotopy invariant of oriented knots and links). The function $\mathbf{f}_{C,\mathsf{c}}$ restricted to the set of oriented knot diagrams $\mathcal{K}$ is closely related to the function $\mathbf{Inv}_C$ of Section 7.1.

A very important example of a cocommutative element is the trace function $\operatorname{Tr} : \mathrm{M}_n(k) \longrightarrow k$ which we regard as an element of $\mathrm{C}_n(k) = \mathrm{M}_n(k)^*$. Since any algebra automorphism t of $\mathrm{M}_n(k)$ is described by $t(x) = GxG^{-1}$ for all $x \in \mathrm{M}_n(k)$, where $G \in \mathrm{M}_n(k)$ is invertible, it follows that Tr is $T_{\mathsf{d}}, T_{\mathsf{u}}$-invariant for all twist oriented quantum coalgebra structures $(\mathrm{C}_n(k), b, T_{\mathsf{d}}, T_{\mathsf{u}})$ on $\mathrm{C}_n(k)$. See the corollary to [**2**, Theorem 4.3.1].

9.1. The Function $\mathbf{f}_{C,\mathsf{c}}$ Defined on Oriented Knot Diagrams. Let c be a $T_{\mathsf{d}} \circ T_{\mathsf{u}}$-invariant cocommutative element of C and suppose that $\mathbf{K} \in \mathcal{K}$. To define the scalar $\mathbf{f}_{C,\mathsf{c}}(\mathbf{K})$ we first construct a functional $\mathbf{f} \in C^*$ as follows. If $\mathbf{K}$ has no crossings set $\mathbf{f} = \epsilon$.

Suppose that $\mathbf{K}$ has $n \geq 1$ crossings. Choose a point P on a vertical line in the knot diagram $\mathbf{K}$. (There is no harm, under regular isotopy, in inserting a vertical

line at the end of a crossing line or local extrema – thus we may assume that $\mathbf{K}$ has a vertical line.) We refer to our chosen point P as the starting point.

Traverse the knot diagram $\mathbf{K}$, starting at P and moving in the direction of the orientation, labelling the crossing lines $1, \dots, 2n$ in the order encountered. For $c \in C$ let $\mathbf{f}(c)$ be a sum of products, where each crossing contributes a factor by the same algorithm which was used to describe $\mathbf{Inv}_C(\mathbf{T})(c)$ in Section 7.1. The proof of Theorem 4 can be repeated verbatim to show that $\mathbf{f}(c)$ is unaffected by the replacement of local parts of the knot diagram $\mathbf{K}$ by their equivalents according to (M.1)–(M.5) and (M.2rev)–(M.5rev).

Let d be the Whitney degree of the oriented knot diagram $\mathbf{K}$. Then $2d$ is the number of local extrema with clockwise orientation minus the number of extrema with counterclockwise orientation. We will show that the scalar

$$(G^d\mathbf{f})(\mathsf{c}) = G^d(\mathsf{c}_{(1)})\mathbf{f}(\mathsf{c}_{(2)})$$

does not depend on the starting point P. Observe to calculate $\mathbf{f}$ we may assume that all crossings are oriented in the upright position. Altering $\mathbf{K}$ to achieve this will not change the Whitney degree. Thus we may assume that all crossings are oriented in the upright position. In light of the proof of Theorem 5 we may also assume that $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}})$ is standard. Set $T = T_{\mathsf{u}}$.

Consider a new starting point P_{new} which precedes P in the orientation of $\mathbf{K}$ and has the property that traversal of the portion of the diagram $\mathbf{K}$ form P_{new} to P in the direction of the orientation passes through exactly one local extremum. Let $\mathbf{f}_{new}$ be the analog of $\mathbf{f}$ constructed for P_{new} and let $m+1, \dots, 2n$ be the labels of the crossing lines between P_{new} and P. Set $r = 1$ if the extremum which precedes P has clockwise orientation and set $r = -1$ otherwise. Then

$$G^d(\mathsf{c}_{(1)})\mathbf{f}(\mathsf{c}_{(2)}) = G^d(\mathsf{c}_{(1)})\mathbf{f}_{new}(\mathsf{c}_{(2)})$$

if

$$\begin{aligned} & G^d(\mathsf{c}_{(1)})T^{\ell_1}(\mathsf{c}_{(2)(1)}) \otimes \cdots \otimes T^{\ell_m}(\mathsf{c}_{(2)(m)}) \otimes \mathsf{c}_{(2)(m+1)} \otimes \cdots \otimes \mathsf{c}_{(2)(2n)} \\ = \quad & G^d(\mathsf{c}_{(1)})T^{\ell_1+r}(\mathsf{c}_{(2)(2n-m+1)}) \otimes \cdots \otimes T^{\ell_m+r}(\mathsf{c}_{(2)(2n)}) \otimes \\ & T^{-2d+r}(\mathsf{c}_{(2)(1)}) \otimes \cdots \otimes T^{-2d+r}(\mathsf{c}_{(2)(2n-m)}) \end{aligned} \tag{16}$$

for all integers $\ell_1, \dots, \ell_m$. We will establish (16) by showing for all $a_1, \dots, a_{2n} \in C^*$ that $a_1 \otimes \cdots \otimes a_{2n}$ applied to both sides of the equation of (16) gives the same result.

Now $t = T^*$ is an algebra automorphism of C^* since T is a coalgebra automorphism of C. The axioms $T^*(G) = G$ and $T(c) = G^{-1} \rightharpoonup c \leftharpoonup G$ for all $c \in C$ translate to $t(G) = G$ and $t(a) = GaG^{-1}$ for all $a \in C^*$. Since c is cocommutative $ab(\mathsf{c}) = ba(\mathsf{c})$ for all $a, b \in C^*$. Let $a_1, \dots, a_{2n} \in C^*$. Applying $a_1 \otimes \cdots \otimes a_{2n}$ to the righthand side of the equation of (16) gives

$$\begin{aligned} & G^d t^{-2d+r}(a_{m+1}) \cdots t^{-2d+r}(a_{2n}) t^{\ell_1+r}(a_1) \cdots t^{\ell_m+r}(a_m)(\mathsf{c}) \\ = \quad & t^r(G^d t^{-2d}(a_{m+1} \cdots a_{2n}) t^{\ell_1}(a_1) \cdots t^{\ell_m}(a_m))(\mathsf{c}) \\ = \quad & G^d G^{-d} a_{m+1} \cdots a_{2n} G^d t^{\ell_1}(a_1) \cdots t^{\ell_m}(a_m)(T^r(\mathsf{c})) \\ = \quad & a_{m+1} \cdots a_{2n} G^d t^{\ell_1}(a_1) \cdots t^{\ell_m}(a_m)(\mathsf{c}) \\ = \quad & G^d t^{\ell_1}(a_1) \cdots t^{\ell_m}(a_m)(a_{m+1} \cdots a_{2n})(\mathsf{c}) \end{aligned}$$

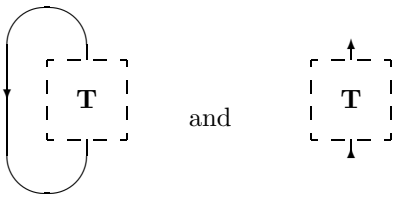
which is $a_1 \otimes \cdots \otimes a_{2n}$ applied to the left hand side of the equation of (16). We have established (16).

Set

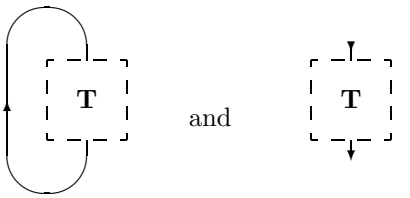
$$\mathbf{f}_{C,\mathsf{c}}(\mathbf{K}) = (G^d\mathbf{f})(\mathsf{c}). \tag{17}$$

The preceding calculations show that (17) describes a well-defined function on $\mathbf{K}$, which by abuse of notation we will refer to as $\mathbf{f}_{C,\mathsf{c}} : \mathcal{K} \longrightarrow k$.

Observe that the oriented knot diagram $\mathbf{K}$ is regularly isotopic to an oriented knot diagram $\mathbf{K}(\mathbf{T})$, where $\mathbf{K}(\mathbf{T})$ is



is an oriented 1–1 tangle diagram, or $\mathbf{K}(\mathbf{T})$ is



is an oriented 1–1 tangle diagram. Since the Whitney degree is a regular isotopy invariant of oriented knot diagrams, the Whitney degrees of $\mathbf{K}$ and $\mathbf{K}(\mathbf{T})$ are the same.

THEOREM 6. *Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}}, G)$ be a twist oriented quantum coalgebra over the field k, let c be a $T_{\mathsf{d}}{\circ}T_{\mathsf{u}}$-invariant cocommutative element of C, and let $\mathbf{f}_{C,\mathsf{c}} : \mathcal{K} \longrightarrow k$ be the function defined by (17).*

a) *Suppose that $\mathbf{K}, \mathbf{K}' \in \mathcal{K}$ are regularly isotopic. Then $\mathbf{f}_{C,\mathsf{c}}(\mathbf{K}) = \mathbf{f}_{C,\mathsf{c}}(\mathbf{K}')$.*

b) *Suppose that $\mathbf{K} \in \mathcal{K}$ and that $\mathbf{K}$ is regularly isotopic to $\mathbf{K}(\mathbf{T})$ for some $\mathbf{T} \in \mathbf{Tang}$. Then*

$$\mathbf{f}_{C,\mathsf{c}}(\mathbf{K}) = (G^d\mathbf{T}_C)(\mathsf{c}),$$

where d is the Whitney degree of $\mathbf{K}$.

c) *$\mathbf{f}_{C,\mathsf{c}}(\mathbf{K}^{op}) = \mathbf{f}_{C^{cop},\mathsf{c}}(\mathbf{K})$ for all $\mathbf{K} \in \mathcal{K}_{\text{knots}}$.*

□

Observe that the formula in part b) of the preceding theorem may be written

$$\mathbf{f}_{C,\mathsf{c}}(\mathbf{K}) = (G^d\mathbf{T}_C)(\mathsf{c}) = \mathbf{T}_C(G^d(\mathsf{c}_{(1)})\mathsf{c}_{(2)}) = \mathbf{T}_C(\mathsf{c}\leftharpoonup G^d).$$

Part c) of the preceding theorem follows with this observation together with the fact that we may assume $\mathbf{K} = \mathbf{K}(\mathbf{T})$ for some $\mathbf{T} \in \mathbf{Tang}^o_{\text{tangles}}$.

Observe that $\mathbf{f}_{C,\mathsf{c}}(\mathbf{K}) = G^d(\mathsf{c})$ when $\mathbf{K}$ has no crossings.

9.2. The function $\mathbf{f}_{C,\mathsf{c}}$ Defined for Oriented Link Diagrams. Let $\mathbf{L} \in \mathcal{L}$ be an oriented link diagram with components $\mathbf{L}_1, \ldots, \mathbf{L}_r$ and suppose that c a $T_{\mathsf{d}}{\circ}T_{\mathsf{u}}$-invariant cocommutative element of the twist oriented quantum coalgebra C. To construct the scalar $\mathbf{f}_{C,\mathsf{c}}(\mathbf{L})$ we modify the procedure for the construction

of $\mathbf{f}_{C,\mathsf{c}}(\mathbf{K})$, where $\mathbf{K} \in \mathcal{K}$ is an oriented knot diagram, described in the preceding section.

For each $1 \leq \ell \leq r$ let d_ℓ denote the Whitney degree of the component $\mathbf{L}_\ell$, let

$$\mathsf{c}(\ell) = \mathsf{c}{\leftharpoonup}G^{d_\ell} = G^{d_\ell}(\mathsf{c}_{(1)})\mathsf{c}_{(2)}$$

and choose a point on a vertical line of $\mathbf{L}_\ell$. We refer to this point as a starting point. (As in the case of knot diagrams we can always assume that each component of $\mathbf{L}$ has a vertical line.) Traverse the component $\mathbf{L}_\ell$, beginning at the starting point and moving in the direction of the orientation, labelling the crossing lines contained in $\mathbf{L}_\ell$ by $(\ell{:}1), (\ell{:}2), \dots$ in the order encountered. Let $u(\ell{:}\imath)$ denote the number of local extrema which are traversed in the counterclockwise direction minus the number of local extrema which are traversed in the clockwise direction during the portion of traversal of the link component from line labelled $(\ell{:}\imath)$ to the starting point.

Next we construct a scalar $\mathbf{f}'_{C,\mathsf{c}}(\mathbf{L})$. If $\mathbf{L}$ has no crossings we set $\mathbf{f}'_{C,\mathsf{c}}(\mathbf{L}) = 1$. Suppose that $\mathbf{L}$ has at least one crossing. Then we define $\mathbf{f}'_{C,\mathsf{c}}(\mathbf{L})$ to be a sum of products, where each crossing contributes a factor of the form

$$\cdots b^{\pm}(T^{\bullet}_{\mathsf{d}} \circ T^{\bullet}_{\mathsf{u}}(\bullet), T^{\bullet}_{\mathsf{d}} \circ T^{\bullet}_{\mathsf{u}}(\bullet)) \cdots$$

according to the conventions of Section 7.1, where $(\ell{:}\imath)$ replaces $\imath$, $(\ell'{:}\imath')$ replaces $\jmath$, and then $\mathsf{c}(\ell)_{(\imath)}$ replaces $c_{(\ell:\imath)}$ and $\mathsf{c}(\ell')_{(\imath')}$ replaces $c_{(\ell':\imath')}$.

We define

$$\mathbf{f}_{C,\mathsf{c}}(\mathbf{L}) = \omega \mathbf{f}'_{C,\mathsf{c}}(\mathbf{L}), \tag{18}$$

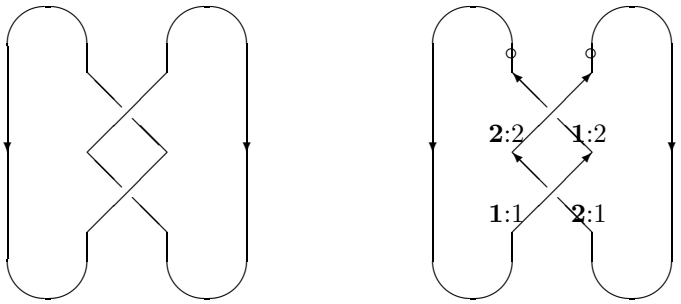
where ω is the product of the $G^{d_\ell}(\mathsf{c})$'s such that the component $\mathbf{L}_\ell$ has no crossing lines. The reader is left with the exercise of showing that $\mathbf{f}_{C,\mathsf{c}}(\mathbf{L})$ does not depend on the particular starting points and is not affected by the replacement of local parts of the diagram $\mathbf{L}$ by their equivalents according to (M.1)–(M.5) and (M.2rev)–(M.5rev). The proof of Theorem 4 provides a blueprint for the latter. Collecting results:

THEOREM 7. *Let $(C, b, T_{\mathsf{d}}, T_{\mathsf{u}}, G)$ be a twist oriented quantum coalgebra over the field k, suppose that c is a $T_{\mathsf{d}} \circ T_{\mathsf{u}}$-invariant cocommutative element of C and let $\mathbf{f}_{C,\mathsf{c}} : \mathcal{L} \longrightarrow k$ be the function described by (18). If $\mathbf{L}, \mathbf{L}' \in \mathcal{L}$ are regularly isotopic then $\mathbf{f}_{C,\mathsf{c}}(\mathbf{L}) = \mathbf{f}_{C,\mathsf{c}}(\mathbf{L}')$.*

□

Observe that $\mathbf{f}_{C,\mathsf{c}}$ restricted to $\mathcal{K}$ is the function described in (17). By virtue of the preceding theorem the function $\mathbf{f}_{C,\mathsf{c}}$ determines a regularly isotopy invariant of oriented links. When C is the dual twist quantum oriented coalgebra of a finite-dimensional twist oriented quantum algebra A over k then the scalar $\mathbf{f}_{C,\mathsf{c}}(\mathbf{L})$ is the invariant $K(L)$ of [**6**] defined for A. See also [**3**].

We end this section with two examples, the Hopf link and the Borromean rings. Consider the oriented Hopf link $\mathbf{L}_{Hopf}$ depicted below left with components $\mathbf{L}_1$ and $\mathbf{L}_2$, reading left to right. The symbol $\circ$ denotes a starting point.

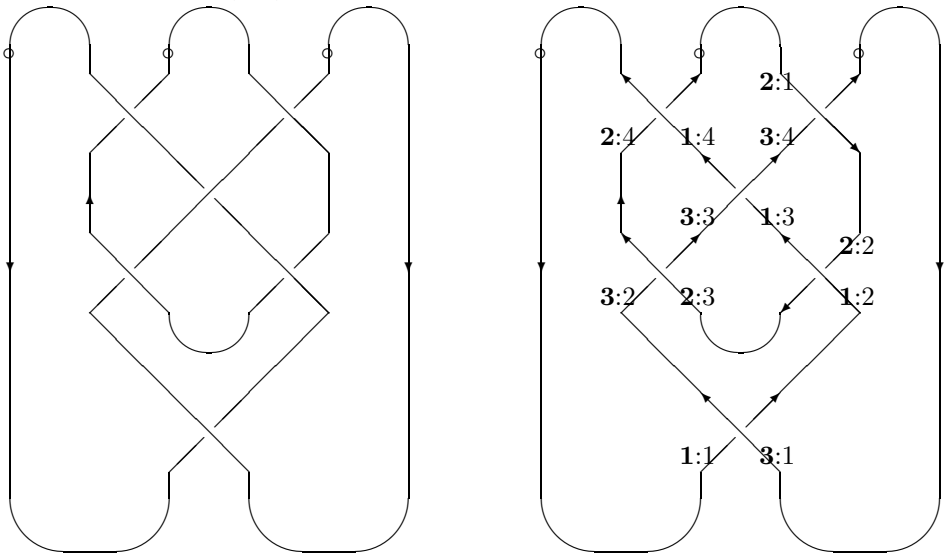


Observe that $d_1 = -1$, $d_2 = 1$ and

$$\mathbf{f}_{C,\mathsf{c}}(\mathbf{L}_{Hopf}) = b(d_{(1)}, e_{(1)})b(e_{(2)}, d_{(2)}),$$

where $d = c \leftharpoonup G^{-1}$ and $e = c \leftharpoonup G$.

Suppose $\mathbf{L}_{\text{Borro}}$ is the Borromean rings with the orientation given in the diagram below left and let $\mathbf{L}_1, \mathbf{L}_2, \mathbf{L}_3$ be the components of $\mathbf{L}_{\text{Borro}}$, reading from left to right.



Observe that $d_1 = -1$, $d_2 = 1 = d_3$ and

$$\mathbf{f}_{C,\mathsf{c}}(\mathbf{L}_{\text{Borro}}) = b^{-1}(e_{(1)}, c_{(1)})b^{-1}(T^2(c_{(2)}), d_{(2)})b(e_{(3)}, c_{(3)}) \times b^{-1}(c_{(4)}, d_{(4)})b^{-1}(d_{(3)}, e_{(2)})b^{-1}(d_{(1)}, e_{(4)})$$

References

[1] V. G. Drinfel'd, Quantum Groups. *Proceedings of the International Congress of Mathematicians,* Berkeley, California, USA (1987), 798–820.

[2] I. N. Herstein, "Noncommutative rings." The Carus Mathematical Monographs, No. 15. Published by The Mathematical Association of America; distributed by John Wiley & Sons, Inc., New York 1968.

[3] Louis Kauffman, Gauss codes, quantum groups and ribbon Hopf algebras. *Reviews in Math. Physics* **5** (1993), 735–773.

[4] Louis Kauffman, "Knots and Physics." World Scientific, Singapore/New Jersey/London/Hong Kong, 1991, 1994.

[5] Louis H. Kauffman and David E. Radford, A separation result for quantum coalgebras with an application to pointed quantum coalgebras of small dimension. *J. Algebra* **225** (2000), 162–200.
[6] Louis H. Kauffman and David E. Radford, Invariants of 3-manifolds derived from finite-dimensional Hopf algebras. *J. Knot Theory Ramifications* **4** (1995), 131–162.
[7] Louis H. Kauffman and David E. Radford, On invariants of knots and links which arise from quantum coalgebras. *in preparation*.
[8] Louis H. Kauffman and David E. Radford, Oriented quantum algebras and invariants of knots and links. *J. Algebra* **246** (2001), 253–291.
[9] Louis H. Kauffman and David E. Radford, Oriented quantum algebras, categories, knots and links. *J. Knot Theory Ramifications* **10** (2001), 1047–1084.
[10] Louis H. Kauffman and David E. Radford, Quantum algebra structures on $n \times n$ matrices. *J. Algebra* **213** (1999), 405–436.
[11] Louis H. Kauffman and David E. Radford, Quantum algebras, quantum coalgebras, invariants of 1–1 tangles and knots. *Comm. Algebra* **28** (2000), 5101–5156.
[12] Larry A. Lambe and David E. Radford, "Introduction to the Quantum Yang–Baxter Equation and Quantum Groups: An algebraic Approach." Kluwer Academic Publishers, Boston/Dordrecht/London, 1997.
[13] S. Montgomery, "Hopf Algebras and their actions on rings." **82**, *Regional Conference Series in Mathematics*, AMS, Providence, RI, 1993.
[14] D. E. Radford, Minimal quasitriangular Hopf algebras. *J. Algebra* **157** (1993), 285–315.
[15] David E. Radford, On parameterized family of twist quantum coalgebras and the bracket polynomial. *J. Algebra* **225** (2000), 93–123.
[16] David E. Radford, On quantum algebras and coalgebras, oriented quantum algebras and coalgebras, invariants of 1-1 tangles, knots and links. *New directions in Hopf algebras*, 263–319, Math. Sci. Res. Inst. Publ., **43**, *Cambridge Univ. Press*, Cambridge, 2002.
[17] N. Yu. Reshetikhin, Quasitriangular Hopf algebras and invariants of links. (Russian) *Algebra i Analiz* **1** (1989), no. 2, 169–188; Translation in *Leningrad Math. J.* **1** (1990), no. 2, 491–513.
[18] N. Yu Reshetikhin and V. G. Turaev, Ribbon graphs and their invariants derived from quantum groups. *Comm. Math. Phys.* **127** (1990), no. 1, 1–26.
[19] M. E. Sweedler, "Hopf Algebras." Benjamin, New York, 1969.

Department of Mathematics, Statistics and Computer Science (m/c 249), 851 South Morgan Street, University of Illinois at Chicago, Chicago, Illinois 60607-7045
E-mail address: kauffman@uic.edu

Department of Mathematics, Statistics and Computer Science (m/c 249), 851 South Morgan Street, University of Illinois at Chicago, Chicago, Illinois 60607-7045
E-mail address: radford@uic.edu

Contemporary Mathematics
Volume **536**, 2011

Space and Time Lattices in Frame Fields of Quantum Representations of Real and Complex Numbers

Paul Benioff

Abstract. Earlier work on reference frame fields based on quantum theory representations of real and complex numbers is expanded here to include space and time lattices in each of the frames. Strings of qudits (d dimensional qubits) are described as hybrid systems in that they are both mathematical and physical systems. The views of systems in a stage j frame, as seen by observers in the stage j frame and in a stage $j-1$ or parent frame are compared. Parent frame views of stage j systems differ in that rational numbers associated with the image systems are states of hybrid systems. Image points of image space and time lattices are tuples of hybrid systems with the state tuples the image point locations. A very brief description of Schrödinger dynamics of image systems on image lattices is given.

1. Introduction

This work has its origin in the need to reach a deeper understanding of the foundational relation between mathematics and physics than is the case at present. The title of Wigner's paper " On the unreasonable effectiveness of mathematics in the natural sciences" [**1**] is still relevant in spite of the large amount of work on this subject. References on this and related questions include [**2, 3**], [**4, 5, 6, 7**] and [**8, 9, 10**]. The work of Tegmark [**9**] is quite explicit in that it suggests that the physical universe is a mathematical universe.

Another approach to this problem is to work towards construction of a theory that treats physics and mathematics together as one coherent whole [**11, 12**]. One would hope that such a theory would show in detail exactly how mathematics and physics are related and why mathematics is so effective in physics. It is possible that both mathematics and physics are so closely intertwined that neither physics nor mathematics can be considered to exist in any a priori sense without the other.

Here an approach to a coherent theory of physics and mathematics is taken that is based on a fields of reference frames that are based on quantum mechanical representations of real and complex numbers [**13, 14**]. The use of reference frames in

1991 *Mathematics Subject Classification.* Primary 81-02, 81P68, 81Q99.

Key words and phrases. quantum real numbers, reference frames, space time lattices.

The author thanks Professors Kazem Mahdavi and Deborah Koslover for the invitation to present this work at the Conference on Interactions between Representation Theory, Quantum Field Theory, Category Theory, and Quantum Information Theory, University of Texas, Tyler, Oct. 1-4, 2009.

physics is not new as is seen from the work in [**15, 16, 17, 18, 19, 20**]. In general, a reference frame provides a background for descriptions of systems. In special relativity, reference frames for describing physical dynamics are based on choices of inertial coordinate systems. In quantum cryptography, polarization directions are used to define reference frames for sending and receiving messages encoded in qubit string states.

As used here reference frames are different in that they are not based on a space time as a background. Instead each reference frame has a mathematical base in that it is based on a quantum theory representation of real and complex numbers. If $R_{j,k,g}, C_{j,k,g}$ denote a specific quantum representation of real and complex numbers, then $F_{j,k,g}$ denotes the reference frame based on $R_{j,k,g}, C_{j,k,g}$.

The indices j, k, g denote the three degrees of freedom associated with quantum representations. One degree, indicated by the integer $k \geq 2$ is common to both classical and quantum representations. It denotes the base for rational numbers as strings of base k digits or qudits where states for each qudit are elements of a k dimensional Hilbert space.

The other two degrees of freedom are present only for quantum representations of numbers. g denotes the basis choice for qudit string states in a Hilbert space and the integer j denotes an iteration stage. The iterations arise because the states of rational number qudit strings, which are used to describe quantum representations of real and complex numbers, are elements of a Fock space that is itself based on real and complex numbers. This leads to the possibility of iteration since quantum representations constructed in a frame can themselves serve as a base of another frame.

Besides $R_{j,k,g}, C_{j,k,g}$, each frame $F_{j,k,g}$ contains mathematical systems that are based on real and complex numbers. Included are the many systems described in texts on mathematical analysis as well as other systems that used real or complex numbers at some point in their description. However physical theories are not yet included because the frames, as described so far, do not contain representations of space and time.

The purpose of this paper is to describe some consequences of inclusion of space and time into each frame. The material presented here will expand on the treatment given elsewhere [**14**] by including some aspects not treated in the earlier work.

Here space and time are included in reference frames as discrete lattices of points. This enables a description of the dynamics and kinematics of representations of physical systems in each frame. Special attention is paid to qudit strings. They are described as hybrid systems in that they are mathematical (their states represent rational numbers) and they are physical (qudit strings are physical systems that have a dynamical and kinematical description).

The view of space and time lattices, qudit string systems, and other physical systems in a frame $F_{j,k,g}$ is contrasted with the view of these stage j systems as seen from a parent stage $j-1$ frame. The difference stems from the position that, to an observer in a frame, the numbers in the real and complex number base of the frame are seen to be abstract and as having no structure other than that required by the relevant axioms.

To an observer in a parent frame, these numbers have structure in that they are equivalence classes of Cauchy sequences of qudit string states. One consequence of this is that the points and point locations of space and time lattices in a frame

are seen in a parent to be tuples and states of qudit string systems. As such they have a dynamics and kinematics. From the parent frame view the points of a child frame lattice move.

The paper continues with the next section devoted to a brief review of the frame field structure based on quantum representations of the real and complex numbers. Next is a section describing space and time lattices in each frame. Then comes a description of qudit strings as hybrid systems, section 4, followed by a description of the parent frame view of child frame entities, section 5.

The paper finishes with a discussion of outstanding issues. Chief among them is the need to merge the frames in the field in some way. This is needed because each frame contains a representation of the physical universe in discrete form; yet there is just one physical universe. Some possible methods of doing this are discussed.

2. Review

Here a brief review of quantum representations of numbers and the resulting reference frame field is given. Emphasis is placed on representations of rational, real, and complex numbers. Details can be found in [**14**].

2.1. Quantum Representations of Numbers.

2.1.1. *Natural Numbers, Integers, and Rational Numbers.* As is well known the natural numbers, the integers and many rational numbers can be represented by finite length strings of base k digits where $k \geq 2$. Rational numbers of the form p/q where p and q contain no prime factors in common and q contains prime factors that are not factors of k are excluded as they are represented by infinite strings of digits that repeat some finite string. For each k the set of numbers so included is denoted by Ra_k. The integers and natural numbers are subsets of rational numbers that have the respective forms $\pm xxxxxxx.$ and $+xxxxxxx.$

Base k quantum representations of these numbers consist of strings of quantum base k digits, or qudits. The state of each qudit is a vector in a k dimensional Hilbert space, $\mathcal{H}_k$, and a string of L qudits is a state in a tensor product space $\mathcal{H}^L$. Qudit string states that correspond to rational numbers have the form

$$|\gamma, s\rangle_{k,L,m,g} = |\gamma, m\rangle_g \bigotimes_{j=1}^{L} |s(j), j\rangle_g. \tag{2.1}$$

Here $s : [1, L] \to \{0, 1, \cdots, k-1\}$ is a $\{0, 1, \cdots, k-1\}$ valued function on the integer interval, $[1, L]$ and $\gamma = +$ or $-$. A compact representation of rational numbers is used here where the position of the sign in the string is also the position of the $k - al$ point. Classical examples of this representation are $-37.42 \to 37 - 42$, $0.073 \to 0 + 073$, $-145 \to 145 -$.

Rational number states of the form of Eq. 2.1 are elements of the product Hilbert space $\mathcal{H}_k^L \bigotimes \mathcal{H}_2$. Here $\mathcal{H}_2$ is the space of the states of the sign qubit.

This description can be extended to include states of qudit strings of arbitrary but finite length. The relevant vector space is a Fock space $\mathcal{F}_k$ which is the direct sum of the product Hilbert spaces

$$\mathcal{F}_k = \bigoplus_L \mathcal{H}_k^L \bigotimes \mathcal{H}_2. \tag{2.2}$$

General states in $\mathcal{F}_k$ are linear superpositions of qudit string states of different length, as in

$$\psi = \sum_{L,m} \sum_{\gamma,s} c_{\gamma,s,L,m} |\gamma, s\rangle_{k,L,m,g} \tag{2.3}$$

The L and m sums are over all positive integers and integers from 0 to L, and the s sum is over all functions with domain $[0, L-1]$.

The subscript g on the states $|\gamma, s\rangle_{k,L,m,g}$ of q_k(qudit) strings denotes a basis choice of states in the Fock space $\mathcal{F}_k$. Because the choice of a basis is arbitrary, there are an infinite number of possible choices. Here the choice of a basis is denoted by the variable g. Since choice of a basis is equivalent to fixing a gauge, g is also a gauge fixing parameter.

Qudit string states of different lengths can also be represented by use of qudit creation and annihilation operators [**13, 22, 23**]. However this will not be done as it is not needed for this paper.

One can also describe gauge and base transformation operators on these states. Gauge transformations correspond to a basis change (g to g') and base transformations correspond to a base change (k to k'). Details are given in [**14**].

2.1.2. *Real and Complex Numbers.* Quantum representations of real numbers are defined as equivalence classes of Cauchy sequences of states of finite q_k strings that are values of rational numbers. Let ψ be a function on the natural numbers such that for each n $\psi(n)$ is a basis state in $\mathcal{F}_k$:

$$\psi(n) = |\gamma_n, s_n\rangle_{k,L_n,m_n,g}. \tag{2.4}$$

For each n the interval $[0, L_n - 1]$ is the domain of s_n and m_n is the position of the sign qubit.

The sequence ψ is a Cauchy sequence if it satisfies the Cauchy condition:

$$\begin{array}{c} \text{For each } \ell \text{ there is a } p \text{ where for all } j, h > p \\ |(|\psi(j) -_{A,k,g} \psi(h)|_{A,k,g})\rangle_{k,g} <_{A,k,g} |+, -\ell\rangle_{k,g}. \end{array} \tag{2.5}$$

Here $|(|\psi(j) -_{A,k,g} \psi(h)|_{A,k,g})\rangle_{k,g}$ is the basis state that is the base k arithmetic absolute value of the state resulting from the arithmetic subtraction of $\psi(h)$ 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, h greater than some p. Here $|+, -\ell\rangle$ is a string state that represents the number $k^{-\ell}$. The subscripts A, k, g in the definition of the Cauchy condition indicate that the operations are arithmetic and are defined for base k string states for the basis choice g. They are *not* the usual quantum theory operations of linear superposition and norm for quantum states.

Equivalence classes of sequences of quantum rational number states are straightforward to define. Sequences ψ and ψ' are in the same equivalence class if the Cauchy condition holds with $\psi(h)$ in Eq. 2.5 replaced by $\psi'(h)$,

The Cauchy condition can be extended to sequences of states that are linear superpositions of basis states. An example is a sequence of states

$$\psi(n) = |\gamma_n, s_n\rangle \otimes (|0_{-n-1}\rangle + |1_{-n-1}\rangle. \tag{2.6}$$

Here $|0_{-n-1}\rangle, |1_{-n-1}\rangle$ are states of a qudit at site $-n-1$. It is clear that this sequence satisfies the Cauchy condition. Also it is different from any classical sequence. More details are given in [**14**].

This example shows that equivalence classes of Cauchy sequences of quantum rational states are larger than classical equivalence classes. However, no new equivalence classes are created.

The quantum representations of real numbers can be easily extended to quantum representations of complex numbers. An obvious method is to represent quantum complex numbers as ordered pairs of quantum real numbers such as $\psi = \psi_R, \psi_I$. ψ_R and ψ_I are each Cauchy sequences of rational number states of base k qudit strings. They also denote the real and imaginary components of ψ. The basic field operations on sequence pairs ψ follow those defined for classical complex numbers.

2.2. Fields of Iterated Reference Frames. As has been seen the definitions of quantum real and complex numbers depend on a choice of a base k for the qudit string states. They have this degree of freedom in common with classical definitions.

However quantum numbers have two degrees of freedom that are not available for classical numbers. One is the choice, g, of a basis set of states in the Hilbert spaces of states for each qudit. The other is a consequence of the fact that the Fock space in which states of qudit strings are described is itself a vector space over the real and complex numbers. It follows that the quantum real and complex numbers can themselves serve as the scalar field for another Fock space. This space can in turn be used to define quantum real and complex numbers.

This leads to an iterative structure in which each representation of real and complex numbers is denoted by $R_{j,k,g}, C_{j,k,g}$ where j denotes the iteration state. Since there are many mathematical systems that can be described as structures base on the real and complex numbers, one can associate a reference frame $F_{j,k,g}$ with each j, k, g that is based on $R_{j,k,g}C_{j,k,g}$. Each $F_{j,k,g}$ contains representations of all mathematical structures that are based on real and complex numbers.

These frames form a field of reference frames parameterized by values of j, k, g [**21, 14**]. The iteration stages can be described in genealogical terms. A stage $j-1$ frame is the parent of a stage j frame. Stage j' frames with $j' > j$ are descendants of a stage j frame. If $j' < j$ the frames are ancestors of a stage j frame.

There are several possibilities for the iteration degree of freedom. The number of iterations can be finite or infinite. If they are infinite, they can be two way infinite, no initial ancestor or terminal defendant, one way infinite, either an initial ancestor and no terminal descendant or no initial ancestor and a terminal descendant. If they are finite they can either have both an initial ancestor and a terminal descendant, or they can be cyclic.

To better visualize the frame field structure it is useful to show some details of the relations between stage j and stage $j+1$ frames. This is provided by Figure 1. The figure shows schematically all stage $j+1$ frames that emanate from a stage j frame. For a given frame, $F_{j,k,g}$, frames with all possible values of g and k are possible children.

An important aspect of the frame field is that, for an observer $O_{j,k,g}$ in $F_{j,k,g}$, the numbers in the real and complex number base of the frame are abstract and featureless. They have no structure other than that required by the relevant axioms for real and complex numbers. However, to an observer O_{j+1} in a parent frame, these numbers have structure as equivalence classes of Cauchy sequences of states of qudit strings. This difference will be important in the following.

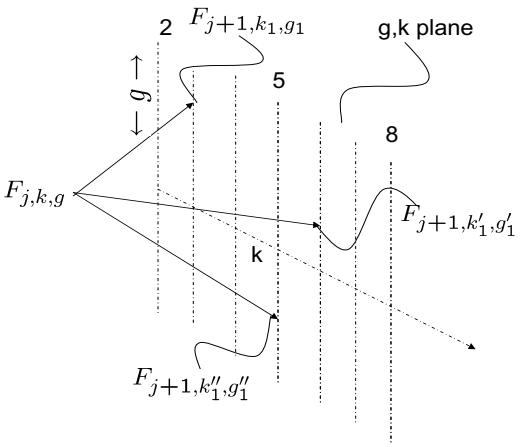


FIGURE 1. Schematic illustration of frames coming from frame $F_{j,k,g}$. Each of the stage $j+1$ frames is based on quantum representations of real and complex numbers as equivalence classis of Cauchy sequences of qudit string states in $F_{j,k,g}$. The distinct vertical lines in the k, g plane denote the discreteness of the integral values of $k \geq 2$. Only three of the infinitely many frames coming from $F_{j,k,g}$ are shown. Here k denotes the qudit base and g denotes a gauge or basis choice.

3. Space and Time Lattices in Reference Frames

One reason for studying quantum numbers is that the resulting reference frame field provides a possible approach to a coherent theory of physics and mathematics together. However the structure of the frames present so far is not sufficient for this purpose in that frame contents are limited to mathematical structures based on real and complex numbers, No physical theories are included and no representations of physical systems are included. The main reason for this lack is that no representations of space and time are included in the frames.

It is proposed to remedy this here by including space and time lattices in each frame. There are several reasons for working with discrete instead of continuous space and time. One reason is that, as will be seen lattices have some interesting properties when viewed from a parent frame. Another is that it is by no means certain that space and time are continuous, especially as the Planck level. Literature that deals with this problem includes work on quantum geometries, [**25, 26, 27, 28, 29**], space time as a foam [**30, 31, 32, 33**], and as a spin network as in loop quantum gravity [**34**]. Space and time may also be emergent in an asymptotic sense [**41**].

For a frame $F_{j,k,g}$ let $\mathcal{L}_{j,k}$ denote the set of space and time lattices in the frame. The lattice in $\mathcal{L}_{j,k}$ all have the form $L_{j,k,L,m}$. As before L is any nonnegative integer and $0 \geq m \geq L$. Each dimension of $L_{j,k,L,m}$ is finite as it contains k^L points with point spacing k^{-m}. If the lattice is D dimensional then it contains k^{LD} points. The point spacing in each direction is the same, at k^{-m}.

The reason for this choice of lattice parameters is that a point location can be expressed by a D tuple of base k rational numbers described by a string of L digits with the $k - al$ point m places from the right end of the string. For instance, if

$L = 5, m = 2$, then the possible locations for each dimension have the form $xxx.xx$ where each x is a base k digit. The restrictions to positive locations is done to simplify the discussion.

The fact that each frame contains many different space and time lattices, one for each value of L and m, is not a problem. This is no different than the usual description of lattices in discrete physics. The only restriction here is that the value of k in $\mathcal{L}_{j,k}$ be the same as that for the real and complex numbers$R_{j,k,g}, C_{j,k,g}$ which are the base of frame $F_{j,k,g}$.

Inclusion of space and time lattices in each frame allows one to include physical theories that describe the kinematics and dynamics of different physical systems on the lattices. In principle, all types of physical systems can be represented. Included are particles, fields, strings, qudit strings, etc. Since the emphasis of this work is the description of qudit strings, the discussion of other types of systems will be quite limited. Also a non relativistic treatment of systems is sufficient here.

4. Qudit Strings as Hybrid Systems

As noted qudit strings are of special interest here. The main reason is that they have both mathematical and physical properties. Their mathematical systems because their states are values of rational numbers. They are physical systems because a string of qudits bound together has mass and a dynamics described by some Hamiltonian. In other words, they are hybrid systems.

Many uses of numbers in physics require that one consider pair, triples, or n tuples of numbers. For example, pairs are needed to to describe complex rational numbers with a real and a imaginary component and D tuples are needed to describe point locations in a D dimensional space and time lattice. If these numbers are to be associated with states of qudit strings, then it is necessary to describe tuples of these hybrid systems. Since single strings are the easiest to treat, they are described first.

4.1. Single Hybrid Systems. A single qudit string, $Q_{k',L,m}$, contains L base k qudits and a sign qubit located m sites from the right end as in $\bar{q}_{[m,L]}\sigma_m\bar{q}_{[1,m]}$. Here $\bar{q}_{[a,b]}$ denotes a string of base k' qudits from string positions a to b and σ_m denotes the sign qubit at site m.

The states of $Q_{k',L,m}$ have the form $|\gamma, \bar{s}\rangle_{k,L,m}$. As before, $\gamma = \pm$ denotes the state of the sign qubit and $\bar{s} : [1, L] \to \{0. \cdots, k' - 1$ gives the state of the qudits in the string. Note that k' can be different from k.

The collection $\mathcal{Q}_{k'}$ contains all strings $Q_{k',L,m}$ for all L, m. The states of these strings represent the values of rational numbers in $Ra_{k'}$. This is the set of all rational numbers expressible as $\alpha \times k^{-m}$ where α is any integer. Note here the distinction between values of rational numbers and rational number systems. Qudit strings are rational number systems whose states in some basis represent values of rational numbers. As such they are mathematical systems.

Qudit strings can also be considered as physical systems consisting of qudits bound together in a string. In particular, $Q_{k',L,m}$, as a string, can be considered as a physical system that has both a kinematic description and a dynamic description. In this sense the qudit strings are hybrid systems in that they are both physical and mathematical systems.

This view of qudit strings is supported by the way they are viewed in physics. In quantum computers qudit strings are physical systems held together by some

external field. An example is the use of linear ion traps that contain systems such as spins that represent the individual qubits [**42**].

Individual qudits can be regarded as both physical systems such as spins or atoms. Or they can be regarded as base k quantum units of information. Their states are physical in that they denote excited states of a system in an external field. The states are also mathematical in that they represent single digit numbers.

The view of qudit strings as hybrid systems can be easily included into the reference frames in a frame field. Let $Q_{j,k',L,m}$ denote a length L string of base k' qudits in a stage j frame $F_{j,k,g}$. m denotes the position of the sign qubit σ. States of the length L strings are elements of a Hilbert space $\mathcal{H}_{j,k'L,m}$.

States of qudit strings of different length belong to a Fock space $\mathcal{F}_{j,k'}$ which is a direct sum over L, m of the $\mathcal{H}_{j,k'L,m}$. Relative to a basis g the states $|\gamma, s\rangle_{j,k',L,m,g}$ denote rational numbers. Often the state subscripts L, m, g will be dropped as they will not be needed.

Physically qudit strings are considered here to be open ended strings. However they can also be considered to be loops or closed strings with no free ends. This suggests that some aspects of string theory [**43**] might be useful to describe the dynamics of these strings.

As a physical system a string in a frame would be expected to have a mass $m_{j,k'L}$ The subscripts k' and L denote the mass dependence on these parameters and j the stage of the frame containing the string. The dynamics of a string $Q_{j,k',L,m}$ in a frame $F_{j,k,g}$ would be described by a Hamiltonian $H^Q_{j,k',L,m}$. Since the string motion is described on a lattice L, j, k, L', m' of three space and one time dimension the Hamiltonian contains difference operators for the kinematic portion.

The Hamiltonian consists of two parts. One describes the center of mass motion of the string and the other describes the states of the qudits in the string.

$$H^Q_{j,k',L,m} = H^Q_{j,CM} + H^{Q_{k',L,m}}_j. \tag{4.1}$$

Hopefully one can choose a physical model for the strings such that rational number states are the eigenstates of $H^{Q_{k',L,m}}_j$. In this case

$$H^{Q_{k',L,m}}_j |\gamma, s\rangle_{j,k',:,m} = E(\gamma, s)|\gamma, s\rangle_{j,k',L,m}. \tag{4.2}$$

Here $E(\gamma, s)$ is the energy of the state $|\gamma, s\rangle_{j,k',L,m}$.

The existence of a Hamiltonian for the hybrid systems means that there is energy associated with the values of rational numbers represented as states of the systems. From this it follows that there are potentially many different energies associated with each rational number value. This is a consequence of the fact that each rational number value has many string state representations that differ by the number of leading and trailing $0s$.

One way to resolve this problem is to let the energy of a hybrid system state with no leading or trailing $0s$ be the energy value for the rational number represented by the state. In this way one has, for each k, a unique energy associated with the value of the rational number for the state. From now on this will be assumed to be the case for $E(\gamma, s)$.

The dependence of $E(\gamma, s)$ on γ, s depends on the physical model used. It would be useful if $E(\gamma, s)$ were proportional to the rational number value represented by the state $|\gamma, s\rangle_{j,k',L,m}$, As energies are bounded from below, one needs to first limit

the proportionality to nonnegative rational number values and then extend it to negative values.

To this end let $\mathcal{H}_{j,k',L,m}$ be a Hilbert space spanned by the states, $|\gamma, s\rangle_{j,k',L,m}$. Let $\tilde{W}$ be a self adjoint operator on $\mathcal{H}_{j,k',L,m}$ that satisfies the eigenvalue equation

$$\tilde{W}|\gamma, s\rangle_{j,k',L,m} = W(\gamma, s)|\gamma, s\rangle_{j,k',L,m} \tag{4.3}$$

where

$$W(\gamma, s) = \gamma \sum_{i=0}^{L-1} s(i)(k')^{i-m}. \tag{4.4}$$

$W(\gamma, s)$ is the number in $R_{j,k,g}$ that corresponds to the rational number value of the state $|\gamma, s\rangle_{j,k',L,m}$.

For $\gamma = +$ define the energy $E(+, s)$ of the state to be proportional to $W(+, s)$ as in

$$E(+, s) = cW(+, s). \tag{4.5}$$

Here c is some constant. There are many ways to extend this proportionality to negative numbers. One would be to have an auxiliary operator for which the sign qubit state is an eigenstate with eigenvalues $= 1, -1$. One can then pair this with the energy eigenstates to obtain

$$\begin{array}{l} +E(+, s) = cW(+, s) \\ -E(-, s) = cW(-, s) \end{array} \tag{4.6}$$

as the eigenvalues of the Hamiltonian and auxiliary operator.

A model that can satisfy Eq. 4.5 has each qudit in a string moving in a one dimensional harmonic potential where the parameter $\omega = \sqrt{d/q}$ depends on the location of the qudit. Here d is the spring constant and q is the qudit mass. The energy levels of a system in such a potential are given by $E_\omega(p) = \omega(p + 1/2)$ for $p = 0, 1, 2, \cdots$.

The qudit position dependence of ω for a qudit string $Q_{j,k',L,m}$ can be obtained by first letting ω_m be the value at site m. For each position i, let ω_i have the value

$$\omega_i = (k')^{i-m}\omega_m. \tag{4.7}$$

To zeroth order, where one neglects the interaction of a qudit with its neighbors or with the neighbor potentials, the spacing of the energy levels of a qudit at site $i+1$ is k' times the spacing of the levels at site i or

$$\Delta E_{i+1} = k'\Delta E_i. \tag{4.8}$$

In this case

$$E_{\omega_i}(k') = k'\Delta E_i = E_{\omega_{i+1}}(1). \tag{4.9}$$

A model for qudit string energies that satisfies Eq. 4.9 has some nice properties. If ψ is a Cauchy sequence of hybrid system states, then the sequence $E(+, s_n)$ of energies converges to a limit $E(+, \psi)$. Here $E(+, \psi(n))$ is the energy associated with the state $\psi(n)$ in the sequence. Also if ψ and ϕ are in the same real number equivalence class, then

$$E(+, \psi) = E(+, \phi). \tag{4.10}$$

4.2. Tuples of Hybrid Systems. Tuples of numbers play an important role in physics. Examples include pairs of real numbers to represent the real and imaginary components of complex numbers, 4 tuples of real numbers to represent space time locations, etc. If these numbers, or rational number approximations of them, are to be represented by states of hybrid systems, then one needs to discuss tuples of hybrid systems.

For complex rational numbers let the pair $Q^{r,i}_{j,k',L,m} = Q_{r,j,k'L,m}, Q_{i,j,k',L,m}$ denote a pair of hybrid systems corresponding to the real and imaginary components of a complex rational number. As a physical system it is desirable that the two component systems are bound into a string pair system. The binding should be sufficiently weak so that the Hamiltonian of the pair system is, to first order, the sum of the Hamiltonians for the two hybrid systems. That is

$$H^{r,i}_{j,k'} = H^{r,i}_{CM,j,k'} + H^{r}_{j,k',L_r,m_r,} + H^{i}_{j,k',L_i,m_i,} + KH^{r,i}_{int}. \tag{4.11}$$

The first term describes the center of mass motion of the hybrid system pair and the next two terms are Hamiltonians for the states of each hybrid system in the pair. The coefficient K in front of the interaction Hamiltonian is sufficiently small so that the term can be neglected to first and higher orders.

In this case, the center of mass motion is independent of the internal states of the two hybrid systems and will be neglected. It follows that the the energy eigenstates of the pair have the form

$$|\gamma_r, s_r\rangle_{r,j,k',L_r,m_r}|\gamma_i, s_i\rangle_{i,j,k',L_i,m_i} \tag{4.12}$$

The corresponding eigenvalue for the pair is the sum of the component eigenvalues,

$$E(\gamma_r, s_r; \gamma_i, s_i) = E(\gamma_r, s_r) + E(\gamma_i, s_i). \tag{4.13}$$

One can extend this to sequences of complex rational number states of hybrid system pairs. Each sequence $\psi(n) = |\gamma_{r,n}, s_{r,n}\rangle_{r,j}|\gamma_{i,n}, s_{i,n}\rangle_{i,j}$ of states can be described as an eigenstate of the nth pair $Q^{r,i}(n)$ in a sequence $Q^{r,i}$ of hybrid system pairs. Depending on the states of the pair systems at different points in the sequence, the state sequence may or may not be a Cauchy sequence. If the sequence is Cauchy in that the real and imaginary components of the sequence are each Cauchy sequences, then the corresponding pair of energy eigenvalue sequences, $E(\gamma_{r,n}, s_{r,n}$ and $\gamma_{i,n}, s_{i,n})$ may or may not converge.

If the strings are such that the real and imaginary sequences of eigenvalues satisfy Eq. 4.9, then the real and imaginary energy eigenvalue sequences converge if and only if the corresponding eigenstate sequences satisfy the Cauchy condition. This would be the case if the individual qudits in sequence of hybrid system pairs moved in a harmonic potential that satisfied Eq. 4.7 and one neglects interactions between neighboring qudits and with potentials other than their own.

A similar description extends to other tuples of numbers and hybrid systems. For example locations of space time points on a lattice are represented by 4 tuples of rational numbers. If these correspond to states of hybrid systems in a weakly bound 4 tuple, then the description for complex rational numbers would apply here too. Each point in a lattice would correspond to a 4 tuple of hybrid systems with the state of the 4 tuple corresponding to the location of the point in the lattice. More details on this will be given later on.

The weak binding of hybrid systems into tuples is supported by states of computers as they would be used in quantum computations using qubits. The matrix of

potential wells that contains N-tuples of qubit string states is tied to the quantum computer. Since the computer is a physical system, it can be translated, rotated, or given a velocity boost. For these transformations the states of the qubit strings in the N-tuples and the space relations of the N qubit strings to one another is unchanged. This would not be the case if two computers collided with one another with sufficient energy to break them up.

5. Frame Entities Viewed from a Parent Frame

The discussion in the last section concentrated on properties of hybrid systems with little attention paid to the frames in which they were located. this needs to be taken into account, particularly if the real and complex numbers in the base of each frame are regarded, by an observer in the frame, as featureless with no structure other than that required by the relevant axioms and resulting theorems.

To be specific let $F_{j,k,g}$ be a frame with real and complex number base $R_{j,k,g}, C_{j,k,g}$. To an observer O_j in the frame the numbers in the frame base are abstract and featureless. The same holds for the locations of points in any space and time lattice, $L_{j,k',L,m}$ in the frame in that the locations are tuples of featureless, abstract rational numbers or they are tuples of real number equivalents of rational numbers. The same property extends to all mathematical structures based on real and complex numbers. For example all numbers appearing in physical theories used to describe the dynamical behavior of physical systems and qudit strings are featureless and abstract.

The view of the contents of a stage j frame is quite different when viewed from a stage $j-1$ parent frame, F_{j-1,k_1,g_1}. An observer O_{j-1} in a parent frame sees the real and complex numbers in the base of the stage j,k (the child) frame as having structure. They are equivalence classes of Cauchy sequences of rational number states of parent frame hybrid systems $Q_{j-1,k,L,m}$.[1]

It is useful to represent these two in-frame views by superscripts j and $j-1$. Thus $R^{j-1}_{j,k,g}, C^{j-1}_{j,k,g}$ and $R^{j}_{j,k,g}, C^{j}_{j,k,g} = R_{j,k,g}, C_{j,k,g}$ denote the stage $j-1$ and stage j frame views of the number base of frame $F_{j,k,g}$. They are often referred to in the following as parent frame images of $R_{j,k,g}, C_{j,k,g}$. Note that the superscript is omitted if it is the same as the subscript.

This can be extended to describe other entities of a frame and their parent frame images. The state

$$\psi_j = \sum_\alpha d^j_{j,\alpha} |\alpha\rangle^j_{j,k,g} \tag{5.1}$$

in $\mathcal{H}^j_{j,k,g}$ corresponds to the state

$$\psi^{j-1}_j = \sum_\alpha d^{j-1}_{j,\alpha} |\alpha\rangle^{j-1}_{j,k,g} \tag{5.2}$$

in $\mathcal{H}^{j-1}_{j,k,g}$, which is the parent frame image of $\mathcal{H}_{j,k,g}$. In the above $d^j_{j,\alpha}$ is a featureless abstract complex number in $C_{j,k,g}$ whereas $d^{j-1}_{j,\alpha}$, as an element of $C^{j-1}_{j,k,g}$, is an equivalence class of Cauchy sequences of pairs of states of parent frame hybrid systems.

[1]The value of k must be the same as the k in $R_{j,k,g}.C_{j,k,g}$.

5.1. Parent Frame Views of Hybrid Systems. The use of stage superscripts and subscripts applies to other frame entities, such as hybrid systems, physical systems, and space and time lattices. A stage j hybrid system $Q_{j,k',L',m'}$ has $Q^{j-1}_{j,k',L',m'}$ as a parent frame image. States, $\gamma', s'\rangle_j$ and $\gamma', s'\rangle^{j-1}_j$ of $Q_{j,k',L',m'}$ and $Q^{j-1}_{j,k',L',m'}$ are, respectively, vectors in $\mathcal{H}_{j,k,g}$ and $\mathcal{H}^{j-1}_{j,k,g}$. The state $|\gamma', s'\rangle_j$ is an eigenstate of a stage j operator, $\tilde{S}_j$, whose corresponding eigenvalue $(\gamma', s')_j$ is a rational real number in $R_{j,k,g}$. As such it has no structure.

The state $|\gamma', s'\rangle^{j-1}_j$ of $Q^{j-1}_{j,k',L',m'}$ is different in that it is an eigenstate of the image, $\tilde{S}^{j-1}_j$, of $\tilde{S}_j$. The eigenvalues, $(\gamma, s)^{j-1}_j$, of $\tilde{S}^{j-1}_j$, are base k rational real numbers in $R^{j-1}_{j,k,g}$. These eigenvalues are equivalence classes of Cauchy sequences of states of sequences, $Q_{j-1,k,L_n,m_n} : n = 1, 2, \cdots$ of hybrid systems in a $j-1$ stage frame.

Since each eigenvalue, $(\gamma, s)^{j-1}_j$, is a base k real rational number the equivalence class for the number contains a constant sequence of a base k rational number. What one would like to accomplish is to associate the base k' rational number eigenvalue $(\gamma, s)^{j-1}_j$, with a constant sequence of base k rational numbers. Then one could equate the eigenvalue $(\gamma, s)^{j-1}_j$ to a state of a single stage $j-1$ hybrid system $Q_{j-1,k.L',m'}$. This would involve equating a constant sequence of base k rational numbers with one element of the sequence.

However, this is possible if and only if the prime factors of k' are prime factors of k. If this is not the case, then the best that can be done is to equate $(\gamma, s)^{j-1}_j$ to a sequence of repeating finite base k states, just as $1/7$ in base 10 is $.142857142857\cdot$.

It follows that image states of image hybrid systems $Q^{j-1}_{j,k',L',m'}$ have image eigenvalues that are base k' rational real numbers in $R^{j-1}_{j,k,g}$. The image eigenvalues correspond to states of stage $j-1$ hybrid systems $Q_{j-1,k,L,m}$ if and only if all prime factors of k' are prime factors of k. The reason is that Cauchy sequences of states of sequences Q_{j-1,k,L_n,m_n}, form the real number base of a stage j frame $F_{j,k,g}$ that contains hybrid systems whose rational number states are $|\gamma, s\rangle_j$ with eigenvalues as numbers in $R_{j,k,g}$.

5.2. Parent Frame Views of Space and Time Lattices. Let $L_{j,k,L,m}$ denote a lattice with 3 space and one time dimension in frame $F_{j,k,g}$. The locations of the lattice points p_j are denoted by 4 tuples of rational numbers with a 3 tuple $\bar{x}_j = x_{i,j}$ for $i = 1, 2, 3$ for the space part and a singleton t_j for the time dimension. As rational number elements of $R_{j,k,g}$, the values of the $x_{i,j}, t_j$ have no structure. They can be represented in the form $\ell_{i,j} \times k^{-m}$, $\ell_{t,j} \times k^{-m}$ where the $\ell i, j, \ell_{t,j}$ are integers whose absolute value is bounded by k^L.

These lattices serve as the space and time arena to describe the motion and dynamics of hybrid systems as well as representations of other types of physical systems in the frame $F_{j,k,g}$. If $\psi^{Q_{j,k',L',m'}}(t_j)$ is the state of a hybrid system $Q_{j,k',L',m'}$ at time t_j the time evolution of the hybrid system state is governed by the Schrödinger equation

$$i\hbar\Delta_t\psi^{Q_{j,k',L',m'}}(t_j) = H^Q_{j,k',L,m}\psi^{Q_{j,k',L',m'}}(t_j). \tag{5.3}$$

The Hamiltonian $H^{Q}_{j,k',L,m}$ is given in Eq. 4.1. The discrete time derivative is given by

$$\Delta_t \psi^{Q_{j,k',L',m'}}(t_j) = \frac{\psi^{Q_{j,k',L',m'}}(t_j + k^{-m}) - \psi^{Q_{j,k',L',m'}}(t_j)}{k^{-m}}. \tag{5.4}$$

k^{-m} is the spacing of adjacent lattice points. It is assumed to be the same for the space and time dimensions. The lattice dynamics of stage j representations, b_j, of other physical systems, denoted collectively here by b, in $F_{j,k,g}$ are described by other Hamiltonians.

A parent frame image, $L^{j-1}_{j,k,L,m}$, of the lattice $L_{j,k,L,m}$ has points p^{j-1}_j whose locations, $\bar{x}^{j-1}_j, t^{j-1}_j$, are $3+1$ tuples of rational numbers in $R^{j-1}_{j,k,g}$. Since the elements of $R^{j-1}_{j,k,g}$ have structure as equivalence classes of Cauchy sequences of stage $j-1$ hybrid systems states, each rational number in $R^{j-1}_{j,k,g}$ is equivalent to a rational number state of a hybrid system.[2] It follows that the image point locations of the image lattice are $3+1$ tuples of rational number states of stage $j-1$ hybrid systems.

This suggests that the points of $L^{j-1}_{j,k,L,m}$ are $3+1$ tuples of hybrid systems. These consist of a triple

$$Q^{\bar{x}}_{j-1,k,L,m} = \bigotimes_{i=1}^{3} Q^{x_i}_{j-1,k,L,m}$$

of space point hybrid systems and a time point hybrid system, $Q^{t}_{j-1,k,L,m}$, bound together as a $3+1$ tuple, $Q^{\bar{x},t}_{j-1,k,L,m}$. The superscripts $\bar{x}, t$ allow for the possibility that the space and time point hybrid systems may have different properties (discussed in more detail later on).

It follows from this view of image lattices that $L^{j-1}_{j,k,L,m}$ consists of k^{4L} $3+1$ tuples of hybrid systems. If each hybrid systems has mass, as a physical system, then the image lattice must be quite massive. This is desirable since one expects space time to be quite rigid.[3]

The properties of a lattice and its parent frame image are shown in Figure 2. The figure shows world lines for a stage j system moving in $L_{j,k,L,m}$ and an image system moving in the image lattice $L^{j-1}_{j,k,L,m}$ for one space and one time direction. The world lines appear the same because they are the same, relative to the points of the lattice and its image.

The use of hybrid systems as rational numbers, points of images of space and time lattices, and as physical systems, may seem strange, especially when viewed from a position outside the frame field and in the usual physical universe. However it is appropriate for a coherent theory of physics and mathematics together as such a theory might be expected to describe systems that are both mathematical and physical systems.

5.3. Energy of Points in Image Lattices. So far the mathematical aspects of hybrid system tuples have been used to represent each image point, p^{j-1}_j, of an image lattice by a 4 tuple $Q^{\bar{x},t}_{j-1,k,L,m}$ of hybrid systems. Here $\bar{x} = x_1, x_2, x_3$ and t

[2] If $\psi(n) = |\gamma, s\rangle_{j,k,L'm'}$ for all n then the sequence $\psi(n)$ is equivalent to $|\gamma, s\rangle_{j,k,L'm'}$.

[3] It cannot be completely rigid because of effects of general relativity that deform flat space time.

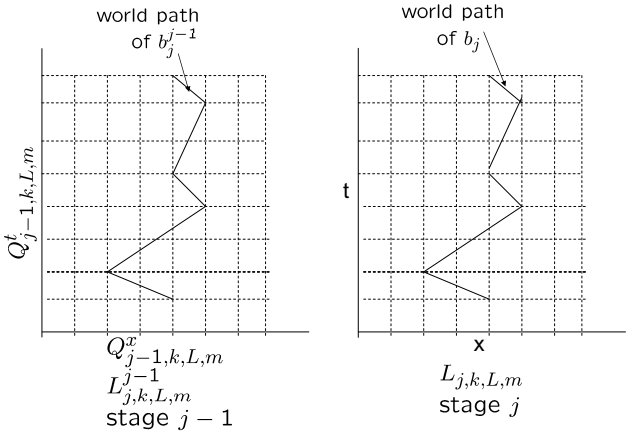


FIGURE 2. Stage j and stage $j-1$ images of one dimensional space and time lattices. Lattice points are indicated by intersections of lines in the two dimensional grid. In $L_{j,k,L,m}$ the points p_j consist of pairs of rational numbers. In $L^{j-1}_{j,k,L,m}$ the image points p_j^{j-1} consist of pairs $Q^x_{j-1,k,L,m}, Q^t_{j-1,k,L,m}$ of hybrid systems with point locations given by the states of the system pairs. Non relativistic world paths of a stage j physical system b_j and of its stage $j-1$ image b_j^{j-1} are shown as solid lines. Note that b can also be a hybrid system.

are labels by which different image points and their components are distinguished. The state of the systems in each tuple corresponds to the location of p^j_{j-1} in the image lattice.

Since each tuple is also a physical system, it has a dynamics described by a Hamiltonian $H^{\bar{x},t}_{j-1,k,L,m}$. This operator describes the motion of the image point 4 tuple on a parent frame space and time lattice $L_{j-1,k',L',m'}$. Following Eq. 4.11, $H_{j-1,k,L,m}$ can be written as a sum of individual qudit string Hamiltonians and an interaction term:

$$H^{\bar{x},t}_{j-1,k,L,m} = \sum_{i=1}^{3} H^{x_i}_{j-1,k,L,m} + H^t_{j-1,k,L,m} + KH^{\bar{x},t}_{int}. \tag{5.5}$$

Here $H^{\bar{x},t}_{int}$ is the interaction Hamiltonian and the constant, K, denotes the strength of the interaction. The term for the center of mass motion for the 4 tuple has been left out as the motion is assumed to be independent of the dynamics of the internal system states.

If K is small, which is assumed to be the case here, then, to first order, the eigenstates of $H^{\bar{x},t}_{j-1,k,L,m}$ can be assumed to be a product of the eigenstates of the Hamiltonians for the component hybrid systems. The energy eigenvalues are then equal to the sum of the energy eigenvalues of the individual components. The eigenvalue equation is

$$\begin{aligned} &H^{\bar{x},t}_{j-1,k,L,m} \bigotimes_{i=1}^{3} |\gamma_{x_i}, s_{x_i}\rangle_{j-1,k} \bigotimes |\gamma_t, s_t\rangle_{j-1,k} \\ &\quad = E(\bar{x},t) \bigotimes_{i=1}^{3} |\gamma_{x_i}, s_{x_i}\rangle_{j-1,k} \bigotimes |\gamma_t, s_t\rangle_{j-1,k} \end{aligned} \tag{5.6}$$

where

$$E(\bar{x},t)=\sum_{i=1}^{3}E(\gamma_{x_i},s_{x_i})+E(\gamma_t,s_t). \tag{5.7}$$

If each point of the image lattice has a dynamics described by Eqs. 5.5, 5.6, and 5.7, then the whole image lattice, $L^{j-1}_{j,k,L,m}$, which consists of $16k^{4L}$ image points (each dimension contains $2k^L-1$ points, neglect the 1) has a Hamiltonian

$$H^{Lat}_{j-1,k,L,m}=\sum_{x_1,x_2,x_3,t}H^{\bar{x},t}_{j-1,k,L,m}+GH^{Lat}_{int,j-1,k,l,m}. \tag{5.8}$$

The sum is over the Hamiltonians for the individual hybrid system tuples for each image lattice point. The constant, G, denotes the strength of the Hamiltonian for the interaction between the different point tuples.

If one neglects the interaction between the different tuples, then the energy eigenvalue equation for the image lattice is

$$H^{Lat}_{j-1,k,L,m}|\gamma^{Lat},s^{Lat}|rangle_{j-1,k,L,m}=E(\gamma^{Lat},s^{Lat})|\gamma^{Lat},s^{Lat}|rangle_{j-1,k,L,m}. \tag{5.9}$$

Here

$$|\gamma^{Lat},s^{Lat}|\rangle_{j-1,k,L,m}=\bigotimes_{\bar{x},t}|\gamma_{\bar{x},t},s_{\bar{x},t}\rangle_{j-1,k,L,m} \tag{5.10}$$

is the $16k^{4L}$ fold product of the states for the individual 4 tuple hybrid systems and

$$E(\gamma^{Lat},s^{Lat})=\sum_{\bar{x},t}E(\gamma_{\bar{x},t},s_{\bar{x},t}). \tag{5.11}$$

The description of the lattice hybrid system tuple Hamiltonian and the states $|\gamma^{Lat},s^{Lat}|\rangle_{j-1,k,L,m}$ describe a large number of independent 4 tuple systems. This is not satisfactory for an image lattice because the $16k^{4L}$ image point location states are all uncorrelated. To be suitable for a lattice the location states must be correlated in that no two of them can be the same. The states must satisfy the condition

$$[\bar{x},t]\neq[\bar{x}',t']\rightarrow|\gamma_{\bar{x},t},s_{\bar{x},t}\rangle_{j-1,k,L,m}\neq|\gamma_{\bar{x},t},s'_{\bar{x}',t}\rangle_{j-1,k,L,m}. \tag{5.12}$$

This condition says that no two image points can have the same location labels.

This is clearly a global correlation because it applies to all image point pairs no matter how different their location labels are. This suggests that the Hamiltonian for the image lattice hybrid system tuples must have this correlation built in. How to accomplish this is an open question and will not be examined further here. However it is worth pointing out that, if the only degrees of freedom available to the lattice 4 tuples are the location states as in Eq. 5.10, then the correlation condition is automatically satisfied if the hybrid systems are fermions. The reason is that the Pauli exclusion principle prohibits any two 4 tuples from being in the same state.

5.4. Dynamics of Image Systems in a Parent Frame. Besides space and time lattices, other systems in a stage j frame have images in a parent stage $j-1$ frame. This includes other types of physical systems, including stage j hybrid systems. Since the emphasis here is on hybrid systems the discussion will be limited to the dynamics of images of stage j hybrid systems.

It should be emphasized that the image $Q^{j-1}_{j,k',L'm'}$ of a stage j system, $Q_{j,k',L'm'}$, is quite different from a stage $j-1$ hybrid system $Q_{j-1,k'',L'',m''}$. The dynamics of the former is described in the image lattice $L^{j-1}_{j,k,L,m}$ and that of the latter is described in a stage $j-1$ lattice L_{j-1,k_1,L_1m_1}.

One sees from this that reference frames are quite cluttered because they contain images of lattices and physical systems of child frames as well as their own lattices and systems. As an aid to understanding the relations between the different systems it is worth showing them in figures. This is done in Figures 3 and 4. Figure 3 shows the contents of a stage j frame and their images in a stage $j-1$ parent frame. Lines indicate the existence of a relationship between the various frame entities. Figure 4 shows the contents of a parent frame, both its own entities and the image entities from a child frame. Lines between entities indicate that the two connected entities are related.

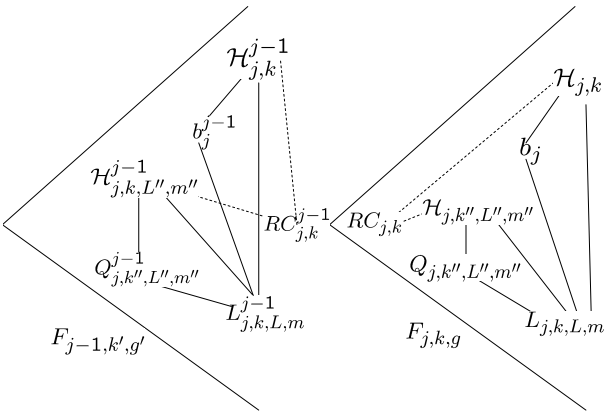


FIGURE 3. Contents of a stage j frame $F_{j,k,g}$ and their images in a parent stage $j-1$ frame, $F_{j-1,k',g'}$. Included are a Lattice, $L_{j,k,L,m}$, a hybrid system, $Q_{j,k''.L''.m''}$, a Hilbert space of states for the hybrid system, $\mathcal{H}_{j,k'',L'',m''}$, a generic physical system, b_j and its Hilbert space of states $\mathcal{H}_{j,k}$, and the frame number base $R_{j,k,g}C_{j,k,g}$. The lines from the systems to the lattices show the space and time lattices in which the systems dynamics take place. The lines to the real and complex numbers show the scalar fields on which the Hilbert spaces are based.

The dynamics of image hybrid systems, $Q^{j-1}_{j,k',L'm'}$ are described in an image lattice, $L^{j-1}_{j,k,L,m}$ whose points and point locations are 4 tuples, $Q^{\bar{x},t}_{j-1,k,L,m}$, of stage $j-1$ hybrid systems. States of the $Q^{j-1}_{j,k',L'm'}$ belong to an image Hilbert space $\mathcal{H}^{j-1}_{j,k',L',m'}$. The dynamics of $Q^{j-1}_{j,k',L'm'}$ interacting with an external image potential is described by a Schrödinger equation with a Hamiltonian

$$H^{Q,j-1}_{j,k',L',m'} = -\frac{\hbar^2}{2M^{Q,j-1}_j}\sum_{i=1}^{3}(\Delta^f)^{j-1}_{j,i,\bar{s}}(\Delta^b)^{j-1}_{j,i,\bar{s}} + V^{j-1}_j(\bar{s}). \tag{5.13}$$

The variable $\bar{s}$ appearing in the discrete derivatives and the potential is a space point location in the image lattice $L^{j-1}_{j,k,L,m}$. It is a stand in for the state $|\bar{\gamma},\bar{s}\rangle_{j-1,k,L,m}$

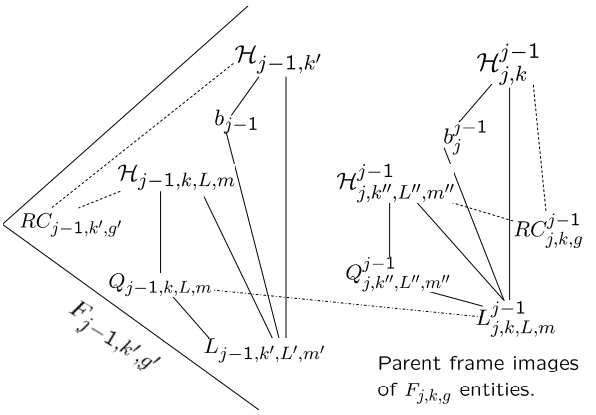


FIGURE 4. The contents of a parent frame $F_{j-1,k',g'}$ are shown. These include the stage $j-1$ systems and entities, and images of the contents of a child frame $F_{j,k,g}$. Other details are given in the caption to the preceding figure. The dotted line connecting the image lattice and the parent frame hybrid system indicates that the points of the image lattice are tuples of parent frame hybrid systems.

of a 3 tuple $Q^{\bar{x}}_{j-1,k,L,m}$ whose rational number states are the locations of the space part of the image points in the lattice. The value of the mass, $2M_j^{Q,j-1}$, of the image hybrid system is a real number in $R^{j-1}_{j,k,g}$ that is expected to be the same as that of $2M_j^Q$, which is the mass of $Q_{j,k',L'm'}$.

The forward and backward discrete derivatives are expressed by

$$(\Delta^f)^{j-1}_{j,i,\bar{s}}\Psi_j^{j-1}(\bar{s},s_t) = \frac{\Psi_j^{j-1}(\bar{s}+\hat{i},s_t)-\Psi_j^{j-1}(\bar{s},s_t)}{\Delta_j^{j-1}}$$

(5.14)

$$(\Delta^b)^{j-1}_{j,i,\bar{s}}\Psi_j^{j-1}(\bar{s},s_t) = \frac{\Psi_j^{j-1}(\bar{s}-\hat{i},s_t)-\Psi_j^{j-1}(\bar{s},s_t)}{\Delta_j^{j-1}}.$$

In these equations $\hat{i}$ denotes the unit vector in the i direction and $\bar{s}+\hat{i}$ denotes the hybrid system state triple $|\gamma_1, s_1 +_A 1\rangle|\gamma_2,s_2\rangle|\gamma_3,s_3\rangle$ for $i=1$. Similar expressions hold for $i=2$ and $i=3$. The subscript A denotes arithmetic addition and subtraction and not linear superposition. For example if $|+,s_1\rangle = |100+111\rangle$ in binary then $|+,s_1+_A 1\rangle = |101+000\rangle$. Also $|+,s_1-_A 1\rangle = |100+110\rangle$. Note that replacing the stand in locations by their equivalents as rational states means that $\Psi_j^{j-1}(\bar{s},s_t) = \Psi_j^{j-1}(|\bar{\gamma},\bar{s}\rangle,|\gamma_t,s_t\rangle)$.

There are many other aspects of the interactions of these hybrid systems and their images that can be examined. However at this point details of these interactions would be speculative and are best left to the future. However, it is worth pointing out that use of states of $Q^{\bar{x}}_{j-1,k,L,m}$ and $Q^t_{j-1,k,L,m}$ as numerical point locations of $L^{j-1}_{j,k,L,m}$ must be reconciled with the physical properties of these systems. As dynamical systems $Q^{\bar{x}}_{j-1,k,L,m}$ and $Q^t_{j-1,k,L,m}$ move and interact with one another and with other physical systems. If these hybrid systems are points and point locations of a space and time lattice image, they must be very stable dynamically

and resistant to change. This suggests that state changing interactions of these systems with each other and with other physical systems must be such that state changes occur very rarely.

6. Discussion

It is worth reemphasizing that this work is only a beginning of a possible approach to a coherent theory of physics and mathematics together. Whether this approach based on reference frame fields is useful or not remains to be seen.

If such an approach is to work, one needs to reconcile the existence of many physical universes, one for each reference frame in the field, with the existence of one physical universe. It is possible that the existence of many universe representations, is related to the various descriptions of multiverses and space time bubbles [**35, 36, 4, 37, 38, 39, 40**]. However, this does not seem likely.

These considerations emphasize the need to merge or combine in some way the different frame representations of physical and mathematical systems. One possible approach is to consider the entities of each frame as different mathematical representations of physical entities. Then one can define physical properties of systems as those which are common to all frame representations. In other words, they are invariant under transformations from one frame to another in the field. These transformations consist of changes in the stage, j, the number base k, and the qudit state basis g [**14**].

The advantage of this approach is that there is no need to merge or combine the frames in the field. They simply are multiple representations of the physical universe. The representation multiplicity arises from the different degrees of freedom available for quantum representations (iteration stage, qudit basis, number base) of real and complex numbers compared to those available for classical representations (number base).

Whether this invariance approach is useful or not remains to be seen. it is also possible that restriction of the type of iteration to the cyclic ones is useful. In this case a descendant frame is also an ancestor frame. This may make it possible for image entities and their properties in a parent frame to be represented in the frame with the original entities.

The use of parent frame hybrid systems to represent space and time points of image space and time lattices suggests that these systems have different properties than other hybrid systems in a frame. For example, for nonrelativistic space and time lattices, the $Q^{\bar{x}}_{j-1,k,L,m}$ systems that represent image space points have different properties than the $Q^{t}_{j-1,k,L,m}$ systems that represent image lattice time points.

These differences in hybrid system types may extend to images of other physical quantities and their measurements. For example, a stage j frame representation of a measurement of a physical quantity P on a quantum system in state ψ to accuracy $\Delta = k^{-m}$ and range $[0, k^{L-m}]$, may have a stage $j-1$ image representation as a stage $j-1$ hybrid system $Q^{P,\psi}_{j-1,k,L,m}$ in a state, $\Psi^{Q,P,\psi}$ that is a linear superposition of rational number states,

$$\Psi^{Q,P,\psi} = \sum_s d_j^{j-1}(s)|+,s\rangle. \tag{6.1}$$

The states $|+, s\rangle$ of $[0, k^{L-m}]$ represent the images of the possible measurement outputs and the coefficients $d_j^{j-1}(s) = \langle +, s|\psi\rangle_j^{j-1}$ are the numbers in $C_{j,k,g}^{j-1}$ that are the same as the numbers $d_j(s)$ in $C_{j,k,g}$, Eq. 5.2.

It is clear that there are many avenues to pursue in future work. These include further development of the use of qudit strings as hybrid systems in physics. It is hoped that they will provide more insight into the nature of a coherent theory of physics and mathematics together. In any case their use in frame fields shows the importance of natural numbers, integers, rational numbers, and real and complex numbers to physics and mathematics.

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, The Unreasonable Effectiveness of Mathematics in the Natural Sciences, *Commum. 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, The Unreasonable Effectiveness of Mathematics, 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. Davies, *The Goldilocks Enigma*, Houghton Mifflin Co., New York, 2006.
5. D. Bendaniel, Linking the Foundations of Physics and Mathematics, ArXiv:math-ph/9907004.
6. S. Wolfram, *A New Kind of Science*, Wolfram Media, Inc. Chanpaign, IL. 2002.
7. C. Chihara, "The Existence of Mathematical Objects", in *Proof and other dilemmas: Mathematics and philosophy*, Bonnie Gold and Roger Simons, Editors, Washington, D.C.: Mathematical Association of America, 2008, pp.131-156.
8. M. Tegmark, Is the Theory of Everything merely the Ultimate Ensemble Theory?, Ann. Phys. (NY), **270**,1,(1998), ArXiv:gr-qc/9704009.
9. M. Tegmark, The Mathematical Universe, Found. Phys. **38**,101-150,(2008), ArXiv:0704.0646.
10. A. Bernal, M. Sánchez, F. Soler Gil, Physics from Scratch. *Letter on M. Tegmark's "The Mathematical Universe"*, ArXiv:0803.0944.
11. P. Benioff, Towards a Coherent Theory of Physica and Mathematics, Found. Phys. **32**,989-1029,(2002), ArXiv:quant-ph/0201093.
12. P. Benioff, Towards a Coherent Theory of Physics and Mathematics: The Theory Experiment Connection, Found. Phys. **35**, 1825-1856, (2005)ArXiv:quant-ph/0403209.
13. P. Benioff, A Representation of Real and Complex Numbers in Quantum Theory, Intl Jour. Pure, Applied Math. **39**, 297-341, (2007), ArXiv:quant-ph/0508219.
14. P. Benioff, Properties of Frame Fields based on Quantum Theory Representations of Real and Complex Numbers, Contemporary Mathematics 482, *Advances in Quantum Computation*, K. Mahdavi and D. Doslover, Eds., September 10-13, 2007, University of Texas, Tyler, TX, pp. 125-163; ArXiv:0709.2664.
15. Y. Aharonov and T. Kaufherr, Quantum frames of reference, Phys. Rev. D **30**, 368-385, (1984).
16. S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Decoherence-full Subsystems and the Cryptographic Power of a Private Shared Reference Frame Phys. Rev. A **70**, 032307 (2004).
17. S. J. van Enk, Quantifying the Resource of Sharing a Reference Frame, Phys. Rev. A **71**, 032339 (2005).
18. S.J. van Enk, Quantum Communication, Reference Frames and Gauge Theory, Phys.Rev. A **73** 042306 (2006), ArXiv:quant-ph/0602079.

19. D. Poulin and J. Yard, Dynamics of a Quantum Reference Frame, New Jour. Phys. **9**, 156, (2007), ArXiv:quant-ph/0612126.
20. S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Reference Frames, Superselection Rules, and Quantum Information, Rev. Mod. Phys. 79, 555-609 (2007).
21. P. Benioff, Fields of Quantum Reference Frames Based on different Representations of Rational Numbers, Jour. Phys. Conference Series, **70**, 012003, (2007). ArXiv:quant-ph/0611139.
22. P. Benioff, The Representation of Numbers in Quantum Mechanics, Algorithmica, **34**, 529-559, (2002), ArXiv:quant-ph/0103078.
23. F. A. Raffa and M. Rasetti, Natural Numbers and Quantum States in Fock Space, ArXiv: 0806.3146.
24. I. Montavy and G. Münster, *Quantum Fields on a Lattice*, Cambridge University Press, Cambridge, UK, (1994).
25. *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.
26. A. Ashtekar, Quantum Mechanics of Geometry, ArXiv:gr-qc/9901023.
27. J. Madore, Noncommutative Geometry for Pedestrians, ArXiv:gr-qc/9906059.
28. A. Connes, *Noncommutative Geometry*, Academic Press, New York, (1994).
29. G. T. Horowitz, Spacetime in String Theory, New Jour. of Physics **7**, 201 (2005), ArXiv:gr-qc/0410049.
30. Y. Jack Ng, Holographic Foam, Dark Energy and Infinite Statistics, ArXiv:gr-qc/0703096.
31. Y. Jack Ng, Spacetime Foam and Dark Energy, ArXiv:0808-1261.
32. G. Amelino-Camelia, Phenomenological Description of Space-Time Foam, ArXiv:gr-qc/0104005.
33. A. A. Kirillov and E. P. Savelova, Spacetime Foam, ArXiv:0806:0443.
34. A. Ashtekar and J. Lewandowski, Background Independent Quantum Gravity: a status report, Classical and Quantum Gravity, **21**, R53-R152, (2004).
35. A.D. Linde, *Inflation and Quantum Cosmology*, Academic Press, Boston 1990.
36. L. Susskind, The Anthropic Landscape of String Theory, ArXiv:hep-th/0302219.
37. P. C. W. Davies, Multiverse Cosmological Models, Mod. Phys. Letters, **A19**, 727-744,(2004), ArXiv:astro-ph/0403047.
38. M. Tegmark, Parallel Universes, in *Science and Ultimate Reality: From Quantum to Cosmos*, J. D. Barrow, P. C. W. Davies, and C. L.Harper, Eds., Cambridge University Press, (2003).
39. D. Deutsch, *The Fabric of Reality*, Allen Lane, New York, (1997).
40. H. Everett, Relative State Formulation of Quantum Mechanics, Rev. of Mod. Phys. **29**, pp 454-462, (1957).
41. N. Seiberg, Emergent Spacetime in *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.
42. D. Kielpinski, C. Monroe, and D. J. Wineland, Architecture for a Large Scale Ion Trap Quantum Computer, Nature, **447**, 709-711, (2002).
43. B. Zweibach, *A First Course in String Theory*, Cambridge Univ. Press, New York, N. Y. 2004.

Physics Division, Argonne National Laboratory,, Argonne, IL 60439, USA
E-mail address: pbenioff@anl.gov

This volume contains a collection of papers, written by physicists, computer scientists, and mathematicians, from the Conference on Representation Theory, Quantum Field Theory, Category Theory, and Quantum Information Theory, which was held at the University of Texas at Tyler from October 1–4, 2009.

Quantum computing is a field at the interface of the physical sciences, computer sciences and mathematics. As such, advances in one field are often overlooked by practitioners in other fields. This volume brings together articles from each of these areas to make students, researchers and others interested in quantum computation aware of the most current advances. It is hoped that this work will stimulate future advances in the field.

ISBN 978-0-8218-4975-0

9 780821 849750

CONM/536