

ARMY RESEARCH LABORATORY



Quantum Computer Circuit Analysis and Design

by Dr. Howard E. Brandt

ARL-TR-4730

February 2009

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory

Adelphi, MD 20783-1197

ARL-TR-4730

February 2009

Quantum Computer Circuit Analysis and Design

Dr. Howard E. Brandt

Sensors and Electron Devices Directorate, ARL

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) February 2009		2. REPORT TYPE Final		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Quantum Computer Circuit Analysis and Design				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Dr. Howard E. Brandt				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Research Laboratory ATTN: AMSRD-ARL-SE-SE 2800 Powder Mill Road Adelphi, MD 20783-1197				8. PERFORMING ORGANIZATION REPORT NUMBER ARL-TR-4730	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Recent developments in the Riemannian geometry of quantum computation offer a new approach to the analysis of quantum computation. A geodesic equation defined on the $SU(2^n)$ group manifold, representing quantum gate operations on n qubits, may be used to determine optimal quantum evolutions and minimum-complexity quantum circuits. The geodesic equation is a first order nonlinear differential matrix equation of the Lax type. This report gives derivations of the Levi-Civita connection, Riemann curvature, sectional curvature, and geodesic equation on the $SU(2^n)$ Riemannian manifold.					
15. SUBJECT TERMS quantum computing, Riemannian geometry, group theory, quantum circuits					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 16	19a. NAME OF RESPONSIBLE PERSON Dr. Howard E. Brandt
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U			19b. TELEPHONE NUMBER (Include area code) 301-394-4143

Contents

Acknowledgments	iv
1. Objective	1
2. Approach	1
3. Results	2
4. Conclusions	6
5. References	7
6. Transitions	8
Distribution List	9

Acknowledgments

I thank the American Mathematical Society for the invitation to present a lecture based on this work as part of a Short Course on Quantum Information and Computation given at the Joint American Mathematical Society (AMS) Meeting 3–4 January 2009 in Washington, DC.

1. Objective

The objective of this project is to perform analyses and designs of efficient fault-tolerant quantum circuits for incorporation in both small- and large-scale quantum computers

2. Approach

Although large-scale quantum computers do not yet exist, future quantum computers have great potential for solving problems beyond the capabilities of classical computers. However, no general methods for constructing new quantum algorithms are known, and potential quantum computer showstoppers presently include only the capabilities of factoring huge numbers and finding a hidden datum in a huge database. Much remains to be discovered concerning the potential power of quantum computers.

Any quantum computation can be ideally represented by a unitary transformation acting in the Hilbert space of the computational degrees of freedom of the quantum computer, and any unitary transformation can be faithfully represented by a network of universal quantum gates, such as two-qubit controlled-NOT (CNOT) gates and single-qubit gates. This is the basis of the quantum circuit model of quantum computation (*I*). The quantum circuit model is the most widely used model of quantum computation. In place of the bits of classical computers, which assign the values 0 or 1, the quantum circuit model is based on qubits, which are quantum systems that can be in a state of 0 or 1 or a quantum superposition of the two, and can be entangled with each other. Qubits may be implemented in a number of possible ways: photon polarization states, atomic states, quantum-dot electron states, Josephson junction charge or flux states, etc. In a quantum computer, the qubits are manipulated by a network of quantum gates in such a way that their final state corresponds to the solution to a computational problem. The quantum gates act on the qubits and can be mathematically represented by tensor products of Pauli matrices.

An important measure of quantum circuit complexity and the difficulty of performing a quantum computation is the number of quantum gates needed. A quantum algorithm is considered efficient if the number of required gates scales only polynomially (not exponentially) with the size of the problem. Quantum circuit networks are usually analyzed using discrete methods; however, potentially powerful continuous differential geometric methods are under development, using Riemannian geometry. Since unitary transformations are themselves continuous, this is perhaps not a surprising development. Using these differential geometric methods, optimal paths in Hilbert space may be found for executing a quantum computation with minimum gate

operations. An appropriate metric, connection, covariant derivative, curvature, and geodesic equation must be formulated.

A new innovative differential geometric approach to quantum circuit complexity was recently introduced by Nielsen et al. (2). A Riemannian metric was formulated on the space of multi-qubit unitary transformations, such that the metric distance between the identity and the desired unitary operator, representing the quantum computation, is equivalent to the number of quantum gates needed to represent that unitary operator, thereby providing a measure of the complexity associated with the corresponding quantum computation. The Riemannian metric can be defined as a positive-definite bilinear form defined in terms of the multi-qubit Hamiltonian. The analytic form of the metric can be chosen to penalize all directions on the manifold not easily simulated by local gates. In this way, basic differential geometric concepts such as the Levi-Civita connection, geodesic path, Riemannian curvature, and geodesic equation can be associated with quantum computation. In accord with the Schrodinger equation, the unitary transformation expressing the quantum evolution is an exponential involving the Hamiltonian. The Hamiltonian can be expressed in terms of tensor products of the Pauli matrices, which act on the qubits. The geodesic equation in the manifold follows from the connection and determines the local optimal Hamiltonian evolution corresponding to the unitary transformation representing the desired quantum computation and minimizing the quantum circuit complexity.

3. Results

A Riemannian metric is first chosen on the manifold of the Lie Group $SU(2^n)$ (special unitary group in 2^n dimensions) of n -qubit unitary operators with unit determinant (3–5). A traceless Hamiltonian serves as a tangent vector to a point on the group manifold of the n -qubit unitary transformation U . The Hamiltonian H is an element of the Lie algebra $su(2^n)$ of traceless $2^n \times 2^n$ Hermitian matrices (3), and is taken to be tangent to the quantum evolutionary curve $e^{-iHt}U$ at $t = 0$. (Here and throughout, I chose units such that Planck's constant divided by 2π is $\hbar = 1$.)

Independent of U , the Riemannian metric (inner product), $\langle \dots \rangle$, is taken to be a positive definite bilinear form $\langle H, J \rangle$ defined on tangent vectors (Hamiltonians) H and J . Following (2), the n -qubit Hamiltonian H can be divided into two parts $P(H)$ and $Q(H)$, where $P(H)$ contains only one and two-body terms, and $Q(H)$ contains more than two-body terms. Thus

$$H = P(H) + Q(H), \quad (1)$$

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

$$P + Q = I, \quad PQ = QP = 0, \quad P^2 = P, \quad Q^2 = Q. \quad (2)$$

For example, in the case of a three-qubit Hamiltonian, for Pauli matrices σ_1, σ_2 , and σ_3 , one has

$$\begin{aligned}
P(H) = & x_1 \sigma_1 \otimes I \otimes I + x_2 \sigma_2 \otimes I \otimes I + x_3 \sigma_3 \otimes I \otimes I + x_4 I \otimes \sigma_1 \otimes I \\
& + x_5 I \otimes \sigma_2 \otimes I + x_6 I \otimes \sigma_3 \otimes I + x_7 I \otimes I \otimes \sigma_1 + x_8 I \otimes I \otimes \sigma_2 \\
& + x_9 I \otimes I \otimes \sigma_3 + x_{10} \sigma_1 \otimes \sigma_2 \otimes I + x_{11} \sigma_1 \otimes I \otimes \sigma_2 + x_{12} I \otimes \sigma_1 \otimes \sigma_2 \\
& + x_{13} \sigma_2 \otimes \sigma_1 \otimes I + x_{14} \sigma_2 \otimes I \otimes \sigma_1 + x_{15} I \otimes \sigma_2 \otimes \sigma_1 + x_{16} \sigma_1 \otimes \sigma_3 \otimes I \\
& + x_{17} \sigma_1 \otimes I \otimes \sigma_3 + x_{18} I \otimes \sigma_1 \otimes \sigma_3 + x_{19} \sigma_3 \otimes \sigma_1 \otimes I + x_{20} \sigma_3 \otimes I \otimes \sigma_1 \\
& + x_{21} I \otimes \sigma_3 \otimes \sigma_1 + x_{22} \sigma_2 \otimes \sigma_3 \otimes I + x_{23} \sigma_2 \otimes I \otimes \sigma_3 + x_{24} I \otimes \sigma_2 \otimes \sigma_3 \\
& + x_{25} \sigma_3 \otimes \sigma_2 \otimes I + x_{26} \sigma_3 \otimes I \otimes \sigma_2 + x_{27} I \otimes \sigma_3 \otimes \sigma_2 + x_{28} \sigma_1 \otimes \sigma_1 \otimes I \\
& + x_{29} \sigma_2 \otimes \sigma_2 \otimes I + x_{30} \sigma_3 \otimes \sigma_3 \otimes I + x_{31} \sigma_1 \otimes I \otimes \sigma_1 + x_{32} \sigma_2 \otimes I \otimes \sigma_2 \\
& + x_{33} \sigma_3 \otimes I \otimes \sigma_3 + x_{34} I \otimes \sigma_1 \otimes \sigma_1 + x_{35} I \otimes \sigma_2 \otimes \sigma_2 + x_{36} I \otimes \sigma_3 \otimes \sigma_3, \quad (3)
\end{aligned}$$

in which \otimes denotes the tensor product, and

$$\begin{aligned}
Q(H) = & x_{37} \sigma_1 \otimes \sigma_2 \otimes \sigma_3 + x_{38} \sigma_1 \otimes \sigma_3 \otimes \sigma_2 + x_{39} \sigma_2 \otimes \sigma_1 \otimes \sigma_3 + x_{40} \sigma_2 \otimes \sigma_3 \otimes \sigma_1 \\
& + x_{41} \sigma_3 \otimes \sigma_1 \otimes \sigma_2 + x_{42} \sigma_3 \otimes \sigma_2 \otimes \sigma_1 + x_{43} \sigma_1 \otimes \sigma_1 \otimes \sigma_2 + x_{44} \sigma_1 \otimes \sigma_2 \otimes \sigma_1 \\
& + x_{45} \sigma_2 \otimes \sigma_1 \otimes \sigma_1 + x_{46} \sigma_1 \otimes \sigma_1 \otimes \sigma_3 + x_{47} \sigma_1 \otimes \sigma_3 \otimes \sigma_1 + x_{48} \sigma_3 \otimes \sigma_1 \otimes \sigma_1 \\
& + x_{49} \sigma_2 \otimes \sigma_2 \otimes \sigma_1 + x_{50} \sigma_2 \otimes \sigma_1 \otimes \sigma_2 + x_{51} \sigma_1 \otimes \sigma_2 \otimes \sigma_2 + x_{52} \sigma_2 \otimes \sigma_2 \otimes \sigma_3 \\
& + x_{53} \sigma_2 \otimes \sigma_3 \otimes \sigma_2 + x_{54} \sigma_3 \otimes \sigma_2 \otimes \sigma_2 + x_{55} \sigma_3 \otimes \sigma_3 \otimes \sigma_1 + x_{56} \sigma_3 \otimes \sigma_1 \otimes \sigma_3 \\
& + x_{57} \sigma_1 \otimes \sigma_3 \otimes \sigma_3 + x_{58} \sigma_3 \otimes \sigma_3 \otimes \sigma_2 + x_{59} \sigma_3 \otimes \sigma_2 \otimes \sigma_3 + x_{60} \sigma_2 \otimes \sigma_3 \otimes \sigma_3 \\
& + x_{61} \sigma_1 \otimes \sigma_1 \otimes \sigma_1 + x_{62} \sigma_2 \otimes \sigma_2 \otimes \sigma_2 + x_{63} \sigma_3 \otimes \sigma_3 \otimes \sigma_3. \quad (4)
\end{aligned}$$

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 $Q(H)$. I exclude the tensor products including only the identity because the Hamiltonian is taken to be traceless. Each of the terms in equations 3 and 4 is an 8×8 matrix. The various tensor products of Pauli matrices, such as those appearing in equations 3 and 4, are referred to as generalized Pauli matrices. In the case of an n -qubit Hamiltonian, there are $4^n - 1$ possible tensor products and each term is a $2^n \times 2^n$ matrix.

The right-invariant Riemannian metric for tangent vectors H and J is given by (2)

$$\langle H, J \rangle \equiv \frac{1}{2^n} \text{Tr}[HG(J)], \quad G = P + qQ. \quad (5)$$

Here the superoperator G is defined in terms of superoperators P and Q , and 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,

$$l = \int_{t_i}^{t_f} dt \langle H(t), H(t) \rangle^{1/2}, \quad (6)$$

and is a measure of the cost of applying a control Hamiltonian $H(t)$ along the path.

Using the metric, equation 5, I derived from first principles and in complete detail (6, 7) the reduced Riemannian metric, inverse metric, the Levi-Civita connection,

$$\Gamma_{\sigma\tau}^{\rho} = \frac{i}{2^{n+1}} \text{Tr}\{G^{-1}(\rho)([\sigma, G(\tau)] + [\tau, G(\sigma)])\}, \quad (7)$$

and the following expression for the covariant derivative of a vector $Z = z^{\sigma} \sigma$ along a vector $Y = y^{\sigma} \sigma$:

$$\nabla_Y Z = y^{\sigma} \partial Z / \partial x^{\sigma} + \frac{i}{2} \{[Y, Z] + G^{-1}([Y, G(Z)] + [Z, G(Y)])\}, \quad (8)$$

in which the Einstein sum convention is understood. In equation 7, Greek letters ρ , σ , and τ denote generalized Pauli matrices appearing in the n -qubit Hamiltonian, and the notation is such that a Greek index (for example, ρ in $\Gamma_{\sigma\tau}^{\rho}$) refers to a particular one of the $4^n - 1$ possible generalized Pauli matrices. An important step in my derivation was to obtain the following identity:

$$\sum_{\sigma} \sigma \text{Tr}(G^{-1}(\sigma)[\tau, G(\lambda)]) = 2^n G^{-1}([\tau, G(\lambda)]). \quad (9)$$

Next considering a curve passing through the origin with tangent vector Y , such that $y^{\delta} = \frac{dx^{\delta}}{dt}$,

it follows from equation 8 that the covariant derivative along the curve in the Hamiltonian representation is given by

$$D_t Z \equiv \nabla_Y Z = \frac{dZ}{dt} + \frac{i}{2} \{[Y, Z] + G^{-1}([Y, G(Z)] + [Z, G(Y)])\}. \quad (10)$$

Because of the right-invariance of the metric, equation 10 is true on the entire manifold. One can next proceed to obtain the geodesic equation. A geodesic in $SU(2^n)$ is a curve $U(t)$ with tangent vector $H(t)$ parallel transported along the curve, namely,

$$D_t H = 0. \quad (11)$$

However, according to equation 10, one has

$$D_t H = \frac{dH}{dt} + \frac{i}{2} \{[H, H] + G^{-1}([H, G(H)] + [H, G(H)])\}, \quad (12)$$

which, when substituting equation 11, becomes

$$\frac{dH}{dt} = -iG^{-1}([H, G(H)]). \quad (13)$$

Next defining

$$L \equiv G(H) \equiv F^{-1}(H), \quad (14)$$

one has

$$\frac{dL}{dt} = \frac{d}{dt} G(H) = G\left(\frac{dH}{dt}\right). \quad (15)$$

Thus substituting equations 13 and 14 in equation 15, one obtains

$$\frac{dL}{dt} = i[L, F(L)]. \quad (16)$$

Equation 14 implies

$$H = G^{-1}(L), \quad (17)$$

and therefore solving equation 16 for L yields the Hamiltonian H producing the geodesic path. Equation 16 is the geodesic equation for the locally optimal quantum computational paths in the $SU(2^n)$ manifold. It is a nonlinear first-order differential matrix equation of the same form as the Lax equation for Lax pairs L and $iF(L)$. Here H and L are $2^n \times 2^n$ matrices, and the superoperator $F = P + q^{-1}Q$.

For the three-qubit case with $P \equiv sS + T$, in which S and T are superoperators projecting out one- and two-body interactions, respectively, and s is a parameter, the solution to the locally optimal Hamiltonian corresponding to the solution of the geodesic equation, equations 16 and 17, is given by

$$H(t) = s^{-1}S_0 + e^{it(q^{-1}-s^{-1})S_0} e^{it(1-q^{-1})(S_0+Q_0)} T_0 e^{-it(1-q^{-1})(S_0+Q_0)} e^{-it(q^{-1}-s^{-1})S_0} + q^{-1} e^{it(q^{-1}-s^{-1})S_0} Q_0 e^{-it(q^{-1}-s^{-1})S_0} \quad (18)$$

where S_0 , T_0 , and Q_0 are the one-, two-, and three-body parts of the initial Hamiltonian.

Also, beginning with equation 7, I derived in complete detail (7, 8) the Riemannian curvature and the sectional curvature of the $SU(2^n)$ group manifold. These quantities are essential for developing increased understanding of the globally optimum quantum computational paths in the $SU(2^n)$ group manifold.

Other work performed, but currently of secondary interest and which because of page limitations is not included in this report, includes the following:

1. A brief survey of the current progress in developing physical implementations of quantum computers and identifying the issues peculiar to each;
 2. Mathematical analyses of quantum circuits for implementing the quantum Fourier transform, expressed in terms of matrix algebra associated with successive stages of the algorithm;
 3. Addressing issues of fault tolerance and the associated requirements for supplementary quantum error correction circuits; and
 4. Determination and analysis of possible quantum circuits for producing generic states of quantum entanglement.
-

4. Conclusions

In this effort, I have derived the necessary differential geometric structure of the $SU(2^n)$ group manifold, including the connection, curvatures, and geodesic equation in complete detail from first principles. This fundamental understanding is essential for the proposed practical applications. It is a necessary step in the design of optimal quantum circuits for implementing small- and large-scale quantum computation. Solutions to the geodesic equation need extensive investigation, keeping in mind that one must incorporate piecewise-smooth joining of local geodesics in order to produce possible global geodesics in the group manifold. Possible conjugate points must be incorporated in the analysis, and possible classical computational obstructions may need to be circumvented in order to facilitate the construction of globally optimum geodesics and associated minimum-complexity circuits for large-scale quantum computation.

5. References

1. Nielsen, M. A.; Chuang, I. L. *Quantum Information and Computation*; Cambridge University Press, 2000.
2. Dowling, M. R.; Nielsen, M. A. The Geometry of Quantum Computation. *Quantum Information and Computation* **2008**, 8, 0861–0899.
3. Pfeifer, Walter *The Lie Algebras $su(N)$* ; Birkhäuser, Basel, 2003.
4. Cornwell, J. F. *Group Theory in Physics, Vols. 1 & 2*; Academic Press, London, 1984.
5. Petersen, P. *Riemannian Geometry*; 2nd Edition, Springer, New York, 2006.
6. Brandt, H. E. Riemannian Geometry of Quantum Computation. To be published in *Nonlinear Analysis* **2008**, 16 pages.
7. Brandt, H. E. Riemannian Geometry of Quantum Computation. AMS Short Course Lecture, *Proceedings of Symposia in Applied Mathematics*, submitted for publication,, American Mathematical Society, Providence, RI, 2009, 35 pages.
8. Brandt, H. E. Riemannian Curvature in the Differential Geometry of Quantum Computation. *Physica E*, submitted for publication, 2009, 8 pages.
9. Brandt, H. E. Differential Geometry of Quantum Computation *J. Modern Optics* **2008**, 55, 3403–3412.
10. Brandt, H. E. Differential Geometry of Quantum Computation. In *Quantum Information and Computation*, SPIE Volume 67976, 69760X-1-10, Bellingham, WA, 2008.

6. Transitions

1. This work will supplement the small U.S. Army Research Laboratory (ARL)-Sensors and Electron Devices Directorate (SEDD) Mission Program on Quantum Computing.
2. I have initiated collaborative research with Dr. John Myers and Prof. Tai Tsun Wu of Harvard University.
3. Five papers have been accepted for publication (four of which are refereed).
4. I presented an American Mathematical Society (AMS) Short Course lecture on this work at AMS Meeting in Washington, DC.
5. I presented work at the Gordon Research Conference on quantum computation.
6. I gave four invited talks at international meetings.
7. I periodically informed a classified Government group of my progress on this research.

No. of Copies	Organization
1 (PDF only)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA 8725 JOHN J KINGMAN RD STE 0944 FORT BELVOIR VA 22060-6218
1	DIRECTOR US ARMY RESEARCH LAB IMNE ALC HR 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB AMSRD ARL CI OK TL 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB AMSRD ARL CI OK PE 2800 POWDER MILL RD ADELPHI MD 20783-1197
11	US ARMY RESEARCH LAB AMSRD ARL SE SE H BRANDT (10 copies) R RAU 2800 POWDER MILL RD ADELPHI MD 20783-1197

ABERDEEN PROVING GROUND

1	DIR USARL AMSRD ARL CI OK TP (BLDG 4600)
---	---

TOTAL: 16 (1 ELEC, 5 CDS, 10 HCs)

INTENTIONALLY LEFT BLANK.