Non-Hermitian quantum gates are more common than Hermitian quantum gates

Anirban Pathak[1,2]

September 17, 2013

[1]Jaypee Institute of Information Technology, A-10, Sector-62, Noida, India

[2]RCPTM, Joint Laboratory of Optics of Palacky University and

Institute of Physics of Academy of Science of the Czech Republic, Faculty of Science, Palacky University, 17. listopadu 12, 771 46 Olomouc, Czech Republic

Abstract

Most of the frequently used quantum gates (e.g., NOT, Hadamard, CNOT, SWAP, Toffoli, Fredkin and Pauli gates) are self-inverse (Hermitian). However, with a simple minded argument it is established that most of the allowed quantum gates are non-Hermitian (non-self-inverse). It is also shown that the % of non-Hermitian gates increases with the dimension. For example, 58.33% of the 2-qubit gates, 98.10% of the 3-qubit gates and 99.99% of the 4-qubit gates are non-Hermitian. As classical reversible gates are essentially permutation gates so the above statistics is strictly valid for classical reversible gates. Further, since Hermiticity is not of much interest in context of the classical reversible gate, hence the result implies that most of the allowed classical reversible gates are non-self-inverse.

Keywords: quantum gates; self-reversible gates; statistcal distribution of quantum gates.

1 Introduction

In last three decades we have observed a major development in the interdisciplinary field of quantum information science. Several interesting phenomena having no classical analogue e.g., quantum teleportation [1], dense coding [2] etc. are introduced. Further, a few quantum algorithms are reported which are faster than the best known classical algorithms for the same tasks [3]. Protocols for unconditionally secure quantum communication are also discovered and implemented [[4, 5] and references therein]. It is interesting to note that to practically utilize the quantum advantages obtained/proposed in the above mentioned protocols and algorithms; we need to realize quantum circuits made up of quantum gates or quantum operations. Quantum gates or quantum operations are linear unitary transformation (with the exception of quantum measurement and here we don't consider measurement as a quantum gate) [6] and therefore are always reversible. This is so because unitarity ensures that if U exists then U^{-1} exists. Thus quantum gates are always reversible. Here we may note that unitarity demands reversibility but it does not demand self reversibility ($U = U^{-1}$). Therefore, we can have both self-inverse and non-self-inverse quantum gates. Reversibility of a gate is not a unique quantum mechanical property. There exists a class of classical reversible gates, too [7]. In fact classical reversible circuits predate quantum circuits. However, with the present understanding of the subject the set of classical reversible gates may be considered as a subset of the set of all quantum gates with a restriction that the inputs and outputs in a classical reversible circuit cannot exist in superposition states. Quantum gates and reversible gates (which is nothing but a restricted special case of quantum

gate) are the essential building blocks for implementing various schemes of quantum and reversible[1] computation [6]. Because of this important role of the quantum and reversible gates, various aspects of quantum and reversible gates are studied in recent past [7, 8, 9, 10, 11, 12]. However, to the best of our knowledge no effort has yet been made to study the statistical distribution of quantum gates. This observation motivated us to address a few very simple but interesting questions. For example: What % of all possible quantum gates are self-inverse? What % of all possible 2-qubit gates are genuinely 2-qubit gates or entangled gates (i.e., cannot be decomposed into single qubit gates)? Present paper aims to address these questions using very simple but mathematically correct logic which does not involve any approximation. The effort leads to very interesting conclusions. Specifically, we have observed that majority of the quantum gates are non-self-inverse i.e., non-Hermitian.

Rest of the paper is organized as follows. In Section 2 we have discussed the condition of self-reversibility and have shown that self-reversibility (or self inverse) implies Hermiticity for unitary operations (gates). In Section 3 we have studied the statistical distribution of quantum gates. Specifically we report the percentages of non-self-inverse quantum gates and genuinely two-qubit quantum gates. Finally we conclude the work in Section 4.

2 Quantum gates and condition for self-reversibility

An m-qubit quantum gate is an unitary operator U that maps an m-qubit state into another m-qubit state. Since a qubit is a two level quantum system, in $\{|0\rangle, |1\rangle\}$ basis we can write an arbitrary qubit as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, where $|\alpha|^2 + |\beta|^2 = 1$ and a single qubit gate as a 2×2 unitary matrix. For example, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a NOT gate. Similarly, in 2^m dimensional Hilbert space a state is a column matrix with 2^m rows, and an m-qubit quantum gate is a $2^m \times 2^m$ unitary matrix. In the previous section we have briefly mentioned several advantages of quantum computing and communication that are reported to date. Implementation of them require quantum gates. The point we wish to establish here is that most of the quantum gates (unitary operators) are non-Hermitian. Thus even within the framework of Hermitian quantum mechanics there exists a topic where non-Hermitian operators are more frequent. To elaborate the idea we will start with some features of quantum gates.

Here we would like to note an interesting feature of quantum gates: An unitary operator A must satisfy $A^{-1} = A^\dagger$ and a Hermitian operator A must satisfy $A = A^\dagger$. Consequently, all unitary operators are not Hermitian and all Hermitian operators are not unitary. If an unitary operator A is Hermitian then $A^{-1} = A^\dagger = A$, i.e., $A = A^{-1}$, so the operator is self inverse. We can easily show the converse (i.e., self inverse unitary operators are Hermitian). We can easily observe that CNOT gate $|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$ is self inverse, so it is Hermitian. Now we can drop the symmetry required for the gate to be self-inverse and modify it to another quantum gate $B = |01\rangle\langle 00| + |11\rangle\langle 01| + |10\rangle\langle 10| + |10\rangle\langle 11|$. Clearly this gate is not self-inverse as $BB|00\rangle = B|01\rangle = |11\rangle \neq |00\rangle$. Clearly this gate is non-Hermitian but interestingly it is unitary.

3 Statistical distributions of quantum gates

Assume that we are working in an M dimensional Hilbert space and the input states are $\{|a_1\rangle, |a_2\rangle, |a_3\rangle, \cdots, |a_M\rangle\}$. Thus $\{|a_i\rangle\}$ forms our input basis set. Similarly assume that $\{|b_j\rangle\}$ represent a new basis set in the same dimension and it is our output basis set. Now we may introduce the operators $U_J = \sum_j |b_j\rangle\langle a_j|$, which are unitary, as is easily verified to satisfy $U_J U_J^\dagger = U_J^\dagger U_J = \left(\sum_p |a_p\rangle\langle b_p|\right)\left(\sum_q |b_q\rangle\langle a_q|\right) = \left(\sum_j |a_j\rangle\langle a_j|\right) = \mathcal{I}_M$. Let Π_J $(J = 1, 2, \cdots, M!)$ be an arbitrary permutation on M letters, each of this permutation will provide us a unitary operator. Each of these $M!$ unitary operators U_J is a quantum gate that always maps input states into mutually orthogonal output

[1]When we refer to a gate as reversible gate it implies that the gate is a classical reversible gate. To specify a quantum gate which is always reversible we referred to the gate as quantum gate.

states. We may call these quantum gates as permutation gates, but these unitary gates are not essentially self-inverse (Hermitian). This fact is elaborated through a specific example in the previous section, where the operator B was unitary but non-self-inverse. Here we would like to note that $\{|b_j\rangle\}$ is only required to be a basis set in M dimension and it is not required to be a permutation of $\{|a_i\rangle\}$. For each unique choice of input basis $\{|a_i\rangle\}$ and output basis $\{|b_j\rangle\}$ we can construct $M!$ quantum gates in M dimension and each of these gates can map input states to mutually orthogonal output states. In essence these are permutation gates.

Permutation gates introduced above can be expressed in a compact notation as follows:

$$U = \begin{pmatrix} |a_1\rangle & |a_2\rangle & \cdots & |a_M\rangle \\ |b_k\rangle & |b_l\rangle & \cdots & |b_n\rangle \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & M \\ k & l & \cdots & n \end{pmatrix} = (k, l, \cdots, n). \tag{1}$$

This notation explicitly identifies the positions occupied by elements before and after application of a permutation gate. The notation uses a matrix, where the states in first row are in $\{|a_i\rangle\}$ and those in the second row are the new arrangement where the states are in $\{|b_i\rangle\}$. Modifying this familiar notation we may now introduce another notation to specify this permutation gate. In our notation numbers in a row indicates new position of the state vectors. For example, $(1, 2, 3, \cdots, M)$ will indicate Identity gate, $(2, 1, 3, 4, 5, \cdots, M)$ will denote a specific permutation gate that maps $|a_2\rangle$ to $|b_1\rangle$, $|a_1\rangle$ to $|b_2\rangle$ and $|a_{i\neq 1,2}\rangle = |b_i\rangle$. Clearly, $(2, 1, 3, 4, 5, \cdots, M)$ is a self inverse gate and thus Hermitian gate. Further, in our compact notation if both input basis and output basis are computational basis then $I_2 = \begin{pmatrix} |0\rangle & |1\rangle \\ |0\rangle & |1\rangle \end{pmatrix} = (1, 2)$ and if the input basis is computational basis and the output basis is diagonal basis $\{|+\rangle, |-\rangle\}$ then the Hadamard gate is $H = \begin{pmatrix} |0\rangle & |1\rangle \\ |+\rangle & |-\rangle \end{pmatrix} = (1, 2)$. Thus with respect to permutation these two gates are equivalent. This would imply that the % of non-Hermitian gates computed below will be valid for each combination of input-output basis sets and the statistical distribution of gates will remain valid in general.

3.1 What % of all possible quantum gates is non-Hermitian (non-self-inverse)?

Now we wish to answer, how many of $M!$ permutation gates obtained for a specific choice of input basis $\{|a_i\rangle\}$ and output basis $\{|b_j\rangle\}$ are Hermitian? As in this context (when we know that the operator/gate is unitary) Hermiticity is equivalent to self inverse. Now Identity gate is always self-inverse. In 2-dimension we can choose two state vectors in ${}^2C_2 = 1$ way and interchange them to form a self inverse gate. In 2-dimension there is only one permutation gate except $(1, 2)$ i.e., $(2, 1)$ and that's self-inverse (it is NOT gate if input basis $\{|a_i\rangle\} = \{|b_j\rangle\}$). Now in 4-dimension we may choose 2 state vectors in ${}^4C_2 = 6$ ways and form following Hermitian gates $(2, 1, 3, 4)$, $(3, 2, 1, 4)$, $(4, 2, 3, 1)$, $(1, 3, 2, 4)$, $(1, 4, 3, 2)$, $(1, 2, 4, 3)$ in addition Identity is a Hermitian gate. Further, we can choose 4 state vectors in pairs of 2 in $\frac{{}^4C_2}{2} = 3$ ways and form the following 3 self inverse gates $(2, 1, 4, 3)$, $(3, 4, 1, 2)$, $(4, 3, 2, 1)$. Thus in total there are $6 + 3 + 1 = 10$ self-inverse (Hermitian) permutation gates in C^4, which includes CNOT $= (1, 2, 4, 3)$ gate. Remaining $4! - 10 = 14$ permutation gates are unitary but non-Hermitian. They are $(2, 3, 1, 4), (2, 3, 4, 1), (1, 3, 4, 2), (1, 4, 2, 3), (2, 4, 1, 3), (2, 4, 3, 1), (3, 1, 2, 4), (3, 1, 4, 2), (3, 2, 4, 1), (3, 4, 2, 1), (4, 1, 2, 3), (4, 1, 3, 2), (4, 2, 1, 3), (4, 3, 1, 2)$. Interestingly, number of possible non-Hermitian permutation gates in C^4 are more than the possible Hermitian gates in C^4. To have a quantitative perception we may note that in C^{2^2}, $\frac{14}{24} \times 100\% = 58.33\%$ of the possible permutation gates are non-Hermitian. Now we need to generalize this idea to C^{2^n}. In order to do so we have to find out the number of self-inverse permutations on M letters, also known as involutions which is denoted as $a[M]$. Involutions or number of alternative permutations is a well studied topic in mathematics. For $M = 1, 2, 3, \cdots$ number of alternating permutations are $a[M] = 1, 2, 4, 10, 26, 76, 232, 764,$ 2620, 9496, 35696, 140152, 568504, 2390480, 10349536, 46206736, 211799312, ...[See Ref. [13] and references therein]. Thus in the context of the present work number of n-qubit Hermitian (self-inverse) gate for a specific choice of input and output bases is $a[2^n]$ and consequently % of non-Hermitian n-qubit quantum gate for that particular combination of input and output basis sets is $r(n) = \frac{(2^n)! - a[2^n]}{(2^n)!} \times 100\%$. As the same ratio would be maintained for all possible combinations of input and output bases so $r(n)$ is the % of non-Hermitian n-qubit quantum gates in

general[2]. Now we can easily check that $r(3) = 98.1052$, $r(4) = 99.9998$. Therefore, 98.10% of the 3-qubit quantum gates and 99.999% of the 4-qubit quantum gates are non-Hermitian. It is interesting to note that most of the possible quantum gates are non-Hermitian and their % increases with the increase in dimension. This is more interesting because most of the popularly used quantum gates (e.g., Hadamard, CNOT, SWAP, Toffoli, Fredkin and Pauli gates) are self-inverse. Only example of non-Hermitian (i.e., non-self-inverse) quantum gate that is popularly used is the phase gate $P(\theta)$ which is in general non-Hermitian except ($P(\pi) = Z$). There is a specific interest in mentioning that $P(\theta)$ is non-Hermitian. We all know that with a beam splitter and a thin-film we can create $P(\theta)$ which implies that non-Hermitian unitary gates are achievable in real experiment. Therefore, we observe that these non-Hermitian quantum gates are not only more prevalent than the Hermitian quantum gates, but are also experimentally realizable.

3.2 What % of all possible 2-qubit quantum gates is entangled gates?

A two-qubit quantum gate that cannot be constructed as a tensor product of two single qubit gates is known as entangled gate. Since such a quantum gate cannot be decomposed into single qubit gates, it is considered as genuinely 2-qubit quantum gate. In other words, the entangled gates are the actual two-qubit gates. To be precise, a unitary gate acting on a bipartite system $A \otimes B$ is called local or separable if $U = U_A \otimes U_B$ where U_A and U_B are single qubit gates. If U cannot be expressed as $U = U_A \otimes U_B$ then the gate is non-local or entangled. The set of any two-qubit entangled gate and all the single qubit gates forms an universal quantum gate library. Thus the entangled two qubits gates are very important. This facts motivates us to ask a question: How frequent are the entangled two qubit gates?

A 2-qubit identity gate is a product of two single qubit identity gate apart from this trivial example there are three other separable gates for a particular choice of input and output basis sets. They are (i) $(1,2) \otimes (3,4) = (3,4) \otimes (1,2)$, (ii) $(1,2) \otimes (4,3) = (4,3) \otimes (1,2)$ and (iii) $(2,1) \otimes (3,4) = (2,1) \otimes (4,3)$. Thus 4 out of 24 two-qubit gates are separable. In other words $\frac{20}{24} \times 100\% = 83.3\%$ of the two qubit gates are entangled gates or genuinely 2-qubits gates that can be used to form universal gate library while combined with the set of all single qubit gates. Thus entangled gates are more common than separable gates and thus almost all two qubit gates may be used to construct universal gate library.

4 Conclusions

Various aspects of quantum gates have been studied since long. However, no effort has yet been made to analyze the statistical distribution of quantum gates from any perspective. Present work provides a fare idea of statistical distribution of quantum gates with respect to (i) Hermitian and non-Hermitian gates and (ii) entangled and non-entangled 2-qubit quantum gates. The outcome of the analysis is interesting from purely foundational as well as application perspective. From the foundational perspective it is extremely interesting to note that the majority of the quantum gates that are allowed by so called Hermitian quantum mechanics are non-Hermitian in nature. Form the application perspective present approach provides some useful idea to design new templates which are expected to be useful in optimizing quantum circuits. To be precise, a template is a quantum (reversible) circuit equivalent to Identity. Templates are known to be useful for optimization of quantum (reversible) circuits [14]. As in the present approach the gates obtained using a fixed input and output bases forms a symmetric group S_N, we can use the group multiplication table to form new templates. For example, if there are N gates we have inverse of all of them in the set so rearrangement theorem tells us that we have N templates of two gates. Now if we wish to convert a particular template $U_1U_2 = I$ into a three gate template, we can keep U_1 fixed and decompose U_2 into two gates and the group rearrangement theorem tells us that the same can be done in N ways, so we have N

[2]It is easy to obtain $r[n]$ using a small Mathematica program: $a[\text{n\_}] = \text{If}[n < 0, 0, n!\text{SeriesCoefficient}[\text{Exp}[x + x\text{\^{}}2/2], \{x, 0, n\}]]; r[\text{n\_}] = \frac{2^n! - a[2^n]}{2^n!} 100.0$. Here the expression for $a[n]$ is used from Ref. [13].

templates of the form $U_1 U_i U_j$. In a similar manner we may generate many simple templates which may be found useful in optimization of quantum circuits.

The fact that most of the quantum gates allowed by quantum mechanics are non-Hermitian is interesting, but it is not surprising. The reason why we don't find it surprising can be clearly understood if we try to physically visualize quantum gates as follows. Time dependent Schrodinger equation is written as $H\psi = i\hbar\frac{d\psi}{dt}$. For our convenience if we consider $\hbar = 1$ then we can write the time evolution of wave function ψ as $\psi(t) = e^{-iHt}\psi(0)$. If we wish to visualize it as a quantum gate then we have to visualize $\psi(0)$ as an input state and $\psi(t)$ as an output state. In that case we have $\psi_{\text{ouput}} = U\psi_{\text{input}}$ where $U = e^{-iHt}$ is an operator which may be visualized as a quantum gate or a quantum circuit that maps an input state $\psi_{\text{input}} = \psi(0)$ into an output state $\psi_{\text{output}} = \psi(t)$. Now we can easily see that the Hermiticity of Hamiltonian H ensures the unitarity of U as $H = H^\dagger$ implies $U^\dagger = e^{+iH^\dagger t} = e^{+iHt}$ and thus $UU^\dagger = U^\dagger U = I$, but it does not necessarily imply $e^{-iHt} = e^{+iHt}$. This clarifies that we can obtain non-Hermitian unitary operators (quantum gates) within the framework of quantum mechanics. This is consistent with our observation. Now in a special situation when a physical Hamiltonian satisfies the condition $e^{-iHt} = e^{+iHt}$ then only the corresponding unitary operator is Hermitian. This situation is really special as it is rare. Specifically, we have seen that 58.33% of the 2-qubit quantum gates, 98.10% of the 3-qubit quantum gates and 99.99% of the 4-qubit quantum gates non-Hermitian.

Acknowledgment: AP thanks Department of Science and Technology (DST), India for support provided through the DST project No. SR/S2/LOP-0012/2010 and he also acknowledges the supports received from the projects CZ.1.05/2.1.00/03.0058 and CZ.1.07/2.3.00/20.0017 of the Ministry of Education, Youth and Sports of the Czech Republic. AP also thanks Dr. A. Banerjee her interest in the work and for some useful technical discussions.

References

[1] C. H. Bennett et al., Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen Channels, Phys. Rev. Lett. **70** (1993) 1895-1899.

[2] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operations on Einstein-Podolsky Rosen states, Phys. Rev. Lett. **69** (1992) 2881-2884.

[3] A. Pathak, Elements of quantum computation and quantum communication, CRC Press, Boca Raton, USA (2013), Chapter 5.

[4] C. Shukla, A. Pathak and R. Srikanth, Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states, Int. J. Quant. Info., **10** (2012) 1241009.

[5] N. Gisin, R. R. Grégoire, T. Wolfgang, and Z. Hugo, Quantum cryptography, Rev. Mod. Phys. **74**, (2002) 145-195.

[6] D. P. DiVincenzo, Quantum gates and circuits, Proc. R. Soc. Lond. A, **454** (1998) 261-276.

[7] M. Saeedi and I. L. Markov, Synthesis and optimization of reversible circuits—a survey, ACM Computing Surveys (CSUR) **45** (2013) 21.

[8] I. L. Markov and M. Saeedi, Faster quantum number factoring via circuit synthesis, Phys. Rev. A **87** (2013) 012310.

[9] D. A. Kronbergc and S. N. Molotkov, Quantum circuit for optimal eavesdropping in quantum key distribution using phase–time coding, J. Experi. Theor. Phys, **111** (2010) 27–56.

[10] Z. Sasanian and D. M. Miller, Reversible and quantum circuit optimization: A functional approach, in Reversible Computation, Lect. Notes Comp. Sc. **7581**, Springer-Verlag Berlin Heidelberg (2013) 112–124.

[11] M. Saeedi, R. Wille and R. Drechsler, Synthesis of quantum circuits for linear nearest neighbor architectures, Quant. Infor. Process **10** (2011) 355–377.

[12] M. Luo, Some quantum states prepared with polynomial quantum circuit, Int. J. Theor. Phys. **51** (2012), 3733–3740.

[13] http://oeis.org/A000085.

[14] D. Maslov, G. W. Dueck and D. M. Miller, Toffoli network synthesis with templates, IEEE Trans. Computer-aided Design Int. Circ. Sys., **24** (2005) 807-817.