The Problem of Testing a Quantum Gate

Subhash Kak

***Abstract*— We consider the question of testing of quantum gates as a part of the larger problem of communication through circuits that use a variety of such gates. We argue that the correct outputs for the basic input values to the two-qubit gate are not sufficient to guarantee satisfactory validation of its workings for all values. We present reasons why these gates may not be error free, and as non-ideal gates they need to be tested for a wide range of probability amplitudes, and we argue that the burden of this additional testing is substantial. Experimental implementations of the controlled-NOT gate have substantial non-unitarity and residual errors. Some analytical results on the complexity of the problem of quantum gate testing are presented.**

***Index Terms*— Non-ideal gates, quantum computing, quantum information, testing a quantum gate**

I. INTRODUCTION

THE problem of testing a quantum gate has no analog in the classical world. Basically, the problem is this: To test a quantum gate we need certified quantum gates to generate all possible inputs and since such gates are not available at this time how are we to certify a gate that has been submitted for certification? Put differently, physical implementations of the gate will be linear only over a restricted range of inputs, whereas quantum computing demands that the gates be completely linear.

To understand the scope of the problem, note that a quantum bit (qubit) $a\,|\,0\rangle + b\,|\,1\rangle$ is different from a classical bit in the sense that it is associated with arbitrary sets of complex values of *a* and *b* as long as $|a|^2 + |b|^2 = 1$. The variables *a* and *b* are probability amplitudes and their mod squares are the probabilities of the component states associated with the qubit. The process of interaction with the qubit causes it to collapse to either $|0\rangle$ or $|1\rangle$ and, consequently, the amount of information that can be extracted from a single qubit is one bit. Unlike a classical state, a quantum state is a superposition of mutually exclusive component states and an unknown quantum state cannot be cloned. Quantum states are also characterized by the Heisenberg Uncertainty Principle. Communication with qubits is of interest to engineers because it represents the use of polarization states of light seen as a stream of single qubits which is appropriate in certain applications using very weak laser outputs. It is also of interest in the problem of quantum cryptography which promises unbreakable security under certain conditions.

The theory of quantum gates is at the basis of quantum computing [1] and just as the hardware for a classical computer is constituted of circuits of logic gates, the practical implementation of a quantum computer is as a circuit made of quantum gates. The problem of testing a quantum gate is, therefore, of interest beyond quantum communication.

In principle the problem of gate testing need not be too restrictive if one can show that the gate works for the widest range of inputs. But in reality the number of inputs to test for increases exponentially as the assumed granularity of data increases. Thus for the case of the Pauli-X gate $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, it is not enough to show that the input $|0\rangle$ become $|1\rangle$ and vice versa and one should be able to establish that the gate transforms $a\,|\,0\rangle + b\,|\,1\rangle$ into $b\,|\,0\rangle + a\,|\,1\rangle$ for *all possible* complex values of a and b. To establish this requires that precise values of can be generated for all *a* and *b* using some other certified gate and then checking the output of the Pauli-X gate being tested. One would need to either use other exact gates to steer the output state to one of the directional bases of the measurement apparatus to confirm this, or to perform a quantum tomographic analysis of the output state [1] that will establish it in a probabilistic sense. It would also be essential to establish that the sum of the squares of the absolute value of the probability amplitudes equals one at the output to ensure that there is no dissipation within the system.

In this paper, we consider the question of testing of quantum gates from the point of view of complexity. We consider implications of a certain desired accuracy at the output of the circuit for the corresponding accuracy of individual gates. Since errors in a linear (or approximately linear) circuit add up, the constraints on individual gates are higher than for the overall circuit. Recent results on the experimental implementations of the controlled-NOT (which is the quantum analog of the classical XOR gate in which the first bit is mod-2 added to the second bit while leaving the first bit unchanged) and the Toffoli gates (CCNOT or universal reversible logic gates) have substantial non-unitarity and residual errors. Since these gates cannot be completely error free, as non-ideal elements they need to be tested for a wide range of probability amplitudes, and the burden of this additional testing is exponential with respect to the number of qubits and quadratic with respect to the desired precision.

Manuscript received September 28, 2012, revised December 4, 2012. This work was supported by National Science Foundation grant #1117068..
Subhash Kak is with the Oklahoma State University, Stillwater, OK, USA (phone: 405-744-6036; fax: 405-744-9097; e-mail: subhash.kak@okstate.edu).

II. Quantum Computing using Gates

Quantum computing has enriched computing theory beyond classical techniques in doing Fourier transform faster (albeit the solution is not fully available), factorization in approximately log *n* rather than $\sqrt{n}$ steps, search for an item with a specific property in an unordered database in roughly $\sqrt{n}$ rather than *n/2* steps, solving Pell's equation (x^2-ny^2=1) in polynomial time, and it has applications to cryptography [1]. But even in theory, quantum computing can only solve problems where the solution amounts a rotation in an appropriate space (as in primality testing since integers form a multiplicative group). The allure of finding new problems that could be shown to be solved faster by quantum algorithms and the challenge of building quantum computing machines has made the field popular amongst mathematicians and physicists. It has also spurred research in materials science and in the experimental area for finding good candidates for implementing quantum circuits.

Given this background, it is worthwhile to investigate prospects for practical quantum computing. Soon after proposals for quantum computing were advanced, it was agreed that problems of decoherence and noise precluded physical implementation of these computers [2]. The implementation had to deal with the following dilemma: The computing system should not interact with the environment lest it decohere, and at the same time it should strongly and precisely interact with the control circuitry. The question of direction of flow of information in a quantum circuit is also an issue. The presence of the arrow of time implies that the system is in a state of non-equilibrium and is, therefore, essentially dissipative [3]. Thus quantum computing itself promotes decoherence and the directionality of information flow implies correlation in the resulting noise associated with the process.

To deal with errors, quantum error correction codes have been proposed although they have not yet been physically implemented. The implementation of these codes would depend on the correct working of very many quantum gates, and, therefore, testing and certifying quantum gates is essential to their effectiveness. There are other questions related to the assumptions under which quantum error correction can be effective, but these questions will not be considered here.

Fault-tolerant conceptual schemes assume that a system could be built recursively (e.g. [4], page 40) where each noisy gate is replaced by an ideal gate by the use of error correction circuitry, but such an idea appears to be impractical. Even if it is assumed that the errors are below a certain threshold, correction in the quantum context can work only if it is related to a known state; in contrast, error correction in classical computation works for unknown states. Certain gate faults, which lie outside of the set of assumptions underlying quantum error correction, cannot be corrected [5].

A non-recursive so-called Fibonacci scheme [6] has been proposed as another approach to quantum error correction. But it assumes the existence of perfect gates in the use of teleportation for error correction. It also uses Bell states, that is two-qubit states in which the qubits are maximally entangled, the generation of which requires the existence of perfect gates. The scheme also assumes that there are no gates with leakage or correlated faults.

It is not possible for this to be true for the quantum case because the unknown received state, for example, could be $a\,|\,0\rangle + b\,|\,1\rangle$ or $c\,|\,0\rangle + e^{i\alpha} d\,|\,1\rangle$, with unknown *a, b, c, d, α,* and if one did not know which one of the two is the correct state, one cannot know what operation is needed on the received state. It may be argued that the initialized state in a quantum computation is known [7], but that cannot be claimed for the intermediate states in the quantum circuit, which would also need to be provided with error correction.

Even assuming that the noise levels are below the threshold associated with the Threshold Theorem and there are enough error-correction resources and the errors are not correlated, there would be the problem of errors introduced before the error correction process begins. There is the additional problem of the presence of gauge states in quantum computing [8].

III. Complexity of testing

Consider a circuit with *k* gates and *n* qubits at input and output. Let the accuracy desired in the output qubits be expressed by δ quantization levels. This means that the error will be ε=1/δ. For example, for the Pauli-X gate with a single qubit $a\,|\,0\rangle + b\,|\,1\rangle$, both *a* and *b* must be associated with δ quantization levels making for a total of δ^2 quantization regions.

Figure 1 represents the situation schematically where the input probability amplitudes *a* and *b* are replaced at the output by new values b^* and a^*. We cannot assume that the circuit is linear over the entire range and, therefore, testing for each of these regions is necessary.

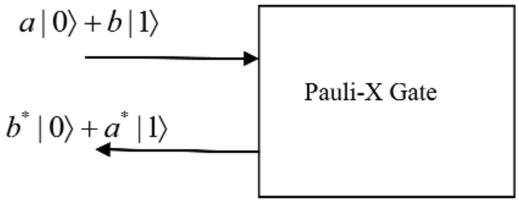
$a\,|\,0\rangle + b\,|\,1\rangle$
$b^*\,|\,0\rangle + a^*\,|\,1\rangle$
Pauli-X Gate

Figure 1. Testing the X gate

Since a real gate will be dissipative to a degree and not be linear over the entire range, it also follows that the square of the estimated probability amplitudes at the output will not equal 1. In other words, $|a^*|^2 + |b^*|^2 \neq 1$.

Theorem 1. The testing of a circuit with n qubits and δ quantization levels is associated with information of n+2 log δ.
Proof. A circuit of n qubits implies a total of 2^n input lines. Since each of these lines has complex input so the total number of quantization levels to be considered is $2^n\delta^2$.

Theorem 2. For a circuit with k stages, the information associated with the testing of each stage is n+2 log kδ.
Proof. Since noise is additive, the accuracy at each stage must be k times better than for the entire circuit.

The amount of testing to be performed at each gate, therefore, is of the order of $2^n k^2 \delta^2$, which is exponential in the number of qubits and quadratic in the number of stages.

Thus for a quantum circuit with 20 qubits and 30 stages, and a desired circuit accuracy of one percent, the amount of testing to be done at each stage for the multi-qubit gate will equal $2^{20} \times 30^2 \times 100^2$. Clearly, for the solution of any meaningful problem, which would require thousands of gates, the constraints on the accuracy of the individual units will be well-nigh impossible to achieve.

IV. EXPERIMENTAL RESULTS ON QUANTUM GATE TESTING

DeMarco *et al* [9] present the best-known implementation of the controlled-NOT gate in which the qubits are the spin and the internal energy (ground and second excited) states of a $^9Be^+$ ion. Table 1 presents the performance and we can see the probabilities do not sum to unity because these data represent the results of four separate experiments.

The fact that checking the performance of the gate in this limited setting itself requires different experiments with different control conditions is symptomatic of the difficulty of testing and it shows that the physical implementation cannot be taken to be an ideal gate.

Table 1: Experimental results of controlled-NOT gate [9]

	↓	↑
n=0	0.989 ± 0.006	0.050 ± 0.007
n=2	0.019 ± 0.007	0.968 ± 0.007

The authors mention errors in the initial state preparation and "limited gate fidelity" as contributing to the less than perfect performance of the gate. Since the probabilities do not add up to one, one can be sure that the behavior of the gate has a dissipative component.

For ease of comparison with the standard gate transformation, one may rewrite the results of Table 1 by representing the internal energy and the spin states in terms of the same qubits as follows:

$$|00\rangle \xrightarrow{CNOT} 0.989\,|00\rangle + 0.050\,|10\rangle$$
$$|10\rangle \xrightarrow{CNOT} 0.019\,|00\rangle + 0.968\,|11\rangle$$

which may be idealized to

$$|00\rangle \xrightarrow{CNOT} |00\rangle$$
$$|10\rangle \xrightarrow{CNOT} |11\rangle$$

Since we don't expect the idealized transformation to be achieved in practice, testing the gate for only two points for a transformation whose range (in terms of the probability amplitudes) is continuous over complex values in the range (0,1) is unsatisfactory. This is like testing the transformation $y=x^2$ for two values of x and taking that to be true for all values.

The correctness of the transformation for two values cannot be extended to other values because we do not know if the experimental arrangement is fully quantum (as the gate is non-ideal) and the influence of the *controlling circuitry cannot be taken to be the same for all values of the probability amplitudes*.

In another implementation of the controlled-NOT gate, based on a string of trapped ions [10] whose electronic states represent the qubits where the control is exercised by focused laser beams, the fidelity of the gate operation *was in the range 70 to 80%* [11]. These were ascribed to laser frequency noise, intensity fluctuations, detuning error, residual thermal excitation, addressing error, and off-resonant excitation. Clearly, this method is not a promising candidate for creating a precise functioning controlled-NOT gate.

For another (c. 2008) optical fiber quantum controlled-NOT gate [12], the authors claim an average logical fidelity of 90% and process fidelity in the range 0.83 to 0.91. The estimated second range is broader because of the substantial errors in the photon sources. Once again the performance is far from ideal.

It is important to note that although the name of the gate is controlled-NOT, the transformation is not that of one input controlling the other in all cases of the input qubits.

As ex-ample, if the input state is $\frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)$ the output state is $\frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)$, in which the first qubit has been transformed under the influence of the second qubit rather than the other way around. In general, we can consider a contolled-NOT gate to be controlled by both the qubits in some proportion, but this is clearly seen only if different superpositions of the qubits are considered.

To test a *non-ideal* controlled-NOT gate, we should be able to show that:

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$
$$\xrightarrow{CNOT} a\,|00\rangle + b\,|01\rangle + c\,|11\rangle + d\,|10\rangle$$

within certain limits of error. In other words, the complex amplitudes (*a, b, c, d*) should map into (*a, b, d, c*) with some small error. It is true if the gate was ideal then testing beyond the two cases of 10 and 11 would not be necessary. But since any physical implementation of the gate would not be ideal, one needs to check the working for the entire range of probability amplitudes to ensure that the errors are within the acceptable threshold.

The testing of the physical gate operating on two qubits requires that various (*a, b, c, d*) amplitudes be generated with perfect fidelity, which requires that a perfectly functioning two-qubit gate (that may be controlled-NOT gate) should already exist. Since each of the values (*a, b, c, d*) is complex and over (0,1) and testing causes collapse to the components along the measurement bases, certification that a quantum gate is in *perfect working order* with no errors whatsoever is *computationally impossible*. It should also be noted that, in contrast, the errors of classical gates are completely correctable.

To test a non-ideal controlled-NOT gate properly, we first need a perfectly functioning controlled-NOT gate to generate a variety of complex superpositions for two qubits. Current experimental evidence on the implementation of the controlled-NOT gate indicate non-unitarity and substantial errors that preclude useful implementations of quantum algorithms.

V. Implementations using Superconducting circuits

Recently, several studies have investigated the use of superconducting circuits for the implementation of quantum gates. In one of these, the implementation of a Toffoli gate was done with three superconducting *transmon* qubits coupled to a microwave resonator [13] where the *transmon* is a type of superconducting charge qubit that has reduced sensitivity to charge noise.

By exploiting the third energy level of the *transmon* qubits, the authors reduced the number of elementary gates needed for the implementation of the gate (that requires six controlled-NOT gates and ten single-qubit operations), relative to that required in theoretical proposals using only two-level systems. Such reduction should have improved the reliability of the gates, but using full process tomography and Monte Carlo process certification, the authors measured fidelity of only 68.5 ± 0:5 per cent.

Another study using superconducting circuits examines the three-qubit code, which maps a one-qubit state to an entangled three-qubit state [14]. The authors implement the correcting three-qubit gate, the conditional-conditional NOT (CCNOT) or Toffoli gate, with a 85±1% fidelity to the expected classical action of this gate and 78 ± 1% fidelity to the ideal quantum process matrix. They also performed a single pass of both quantum bit- and phase-flip error correction with 76 ± 0.5% process fidelity.

In the above-mentioned studies the results, for the most basic testing of the gate, are thus disappointing. One reason behind this performance may be the statistical constraints that need be satisfied [15].

VI. Comparing classical and quantum paradigms

The difficulties of gate testing are another manifestation of the fact that the quantum computing paradigm is fundamentally different from the classical one. This may be seen in the consideration of quantum teleportation, which is transporting an unknown quantum state to a remote location using Bell states and classical communication. While mathematically it is easy to show that quantum teleportation works, there is no way one can certify that a given unknown state has been teleported correctly. The pair of resource qubits in Bell correlation in the experimental arrangement may not be correctly entangled and the gates may also have errors. Furthermore, a customer may not be sure that a specific quantum object supplied to him by the Certification Authority is not entangled with some other object. The fact that quantum mechanics is not a theory of individual objects but rather of collectives [16] has unexpected consequences for certification of transactions in an information network.

A quantum system composed of several subsystems can be in an entangled state, in which the properties of the full system are well defined but the properties of each subsystem are not well defined. This is also the reason why it is difficult to account for quantum mechanical effects in biological system [17]-[20].

The difficulty of implementing quantum gates (and of testing them) creates substantial burdens in the practical realization of the quantum circuit model of computing. It is no wonder that progress in physical implementations is limited and there is no unanimity on what kind of physical qubits to use [6].

Unlike classical computing, we cannot test the performance of given quantum gates while using imprecise signal generators because the requirement of linearity should hold over all possible values [21]. The time taken for a gate to operate creates another complication in a concatenation of gates. For example, the time taken was 63 ns in the superconducting circuit implementation of a CCNOT gate. Furthermore, the gate times are not constants and thus the propagation of qubits in the quantum circuit will suffer from timing issues [22].

In a classical circuit the accuracy of individual gates can be less than that of the entire circuit and we can create a reliable circuit using relatively less reliable component gates [23]. The extension of this for quantum processing is true in a very restrictive sense. In quantum computing the threshold theorem claims that a noisy quantum computer can accurately and efficiently simulate any ideal quantum computation provided that noise is weakly correlated and its strength is below the critical quantum accuracy threshold. But there is no evidence that errors in quantum gates fall below this threshold and that noise is only weakly correlated [24]-[27].

Given that the sources of errors in the gates are many that interact in a variety of modes, one might suppose that a threshold is associated with an error parameter ε so that below ε_0 the error is linear but above ε_0 it becomes uncontrollable large. Such a consideration is meaningful in classical computing where one can estimate in advance, or otherwise limit, the range of signals that drive the computation. No such limit can be assigned for quantum computing as the probability amplitudes, in principle, have all possible values – with no constraints on phase values – so long as their absolute value remains less than one.

VII. Conclusions

We conclude that the representational difference between classical and quantum states has the most profound implications for their circuit implementations. Mapping classical bits into corresponding qubits increases the representation space by virtue of the complex probability amplitudes that get associated with the component states and their superposition. While this provides advantages in the solution of certain problems, it also creates new difficulties in the control and testing of quantum hardware.

If using quantum circuits one can, in principle, solve an exponential number of problems at the same time (although the solution to only one of these may be accessed), it also increases the size of the control space exponentially. The problems of controlling a quantum gate and testing it become correspondingly harder. Quantum computing systems do not scale. What quantum mechanics giveth by one hand, it taketh away by another.

References

[1] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[2] R. Landauer, The physical nature of information. Phys. Lett. A 217, 188- 193, 1996.

[3] D.K. Ferry, Quantum computing and probability. J. Phys.: Condens. Matter 21 474201, 2009.

[4] P. Aliferis, Level Reduction and the Quantum Threshold Theorem. Ph.D. Thesis, Caltech, 2007; arXiv:quant-ph/0703230v1

[5] S. Kak, Information complexity of quantum gates. Int. Journal of Theoretical Physics 45: 933-941, 2006.

[6] P. Aliferis and J. Preskill, The Fibonacci scheme for fault-tolerant quantum computation. arXiv:0809.5063

[7] S. Kak, The initialization problem in quantum computing. Foundations of Physics 29: 267-279, 1999.

[8] A. Bruno, A. Capolupo, S. Kak, G. Raimondo and G. Vitielli, Gauge theory and two level systems. Mod. Phys. Lett. B, vol. 25, pp. 1661-1670, 2011.

[9] B. DeMarco, A. Ben-Kish, D. Leibfried,V. Meyer, M. Rowe, B.M. Jelenkovic, W.M. Itano, J. Britton, C. Langer, T. Rosenband, and D. J. Wineland, Experimental demonstration of a controlled-NOT wave-packet gate. Phys. Rev. Lett. 89: 267901-1-4, 2002.

[10] J.I. Cirac and P. Zoller, Quantum computations with cold trapped ions. Phys. Rev. Lett. 74: 4091-4094, 1995.

[11] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner and R. Blatt, Realization of the Cirac-Zoller controlled-NOT quantum gate. Nature 422: 408-411, 2003.

[12] A.S. Clark, J. Fulconis, J.G. Rarity, W.J. Wadsworth, J.L. O'Brien, An all optical fibre quantum controlled-NOT gate. arXiv:0802.1676

[13] A. Fedorov, L. Steffen, M. Baur, M.P. da Silva, and A. Wallraff, Implementation of a Toffoli gate with superconducting circuits. Nature 481, 170, 2012.

[14] M. D. Reed, L. DiCarlo, S. E. Nigg, L. Sun, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, Realization of three-qubit quantum error correction with superconducting circuits. Nature 482, 382, 2012.

[15] S. Kak, Statistical constraints in starting a quantum computation. Pramana, Journal of Physics 57: 683-688, 2001.

[16] A. Peres, Quantum Theory: Concepts and Methods. Springer, 1995.

[17] S. Kak, The three languages of the brain: quantum, reorganizational, and associative. In: K. Pribram and J. King (editors), Learning as Self-Organization. Lawrence Erlbaum, Mahwah, 185–219, 1996. .

[18] S. Kak, Active agents, intelligence, and quantum computing. Information Sciences 128: 1-17, 2000.

[19] M.I. Franco, L. Turin, A. Mershin, E.M.C. Skoulakis, Molecular vibration-sensing component in Drosophila melanogaster olfaction. Proceedings of the National Academy of Sciences of the USA 108: 3797–3802, 2011.

[20] P. Ball, The dawn of quantum biology. Nature 474: 272-274, 2011.

[21] S. Kak, Information, physics and computation. Foundations of Physics 26: 127-137, 1996.

[22] S. Ashhab, P. C. de Groot, F. Nori, Speed limits for quantum gates in multi-qubit systems. Phys. Rev. A 85, 052327, 2012.

[23] J. von Neumann, Probabilistic logics and the synthesis of reliable organisms from unreliable components. In C. E. Shannon and J. McCarthy, editors, Automata Studies, volume 3, pages 43–99. Princeton University Press, Princeton, 1956.

[24] R. Alicki, Quantum memory as a perpetuum mobile? Stability v.s. reversibility of information processing. Open Systems & Information Dynamics 19, 2012.

[25] G. Kalai, How quantum computers fail: Quantum codes, correlations in physical systems, and noise accumulation. arXiv:1106.0485

[26] M. Dyakonov, Is fault-tolerant quantum computation really possible? In: Future Trends in Microelectronics. Up the Nano Creek, S. Luryi, J. Xu, and A. Zaslavsky (eds), pp. 4-18, Wiley, 2007.

[27] M. Dyakonov, Revisiting the hopes for scalable quantum computation. arXiv:1210.1782

Subhash Kak is Regents Professor and Head of the Department of Computer Science at Oklahoma State University at Stillwater. Prior to joining Oklahoma State University, he served for many years as the Delaune Distinguished Professor of Electrical and Computer Engineering at Louisiana State University in Baton Rouge. He is the author of several books that include The Nature of Physical Reality (New York, Peter Lang, 1986) and The Architecture of Knowledge (New Delhi, CRC, 2004). His areas of interest include data security, quantum computing, information theory, neural networks, and history of science.

Professor Kak's awards include British Council Fellow (1976), Science Academy Medal of the Indian National Science Academy (1977), Kothari Prize (1977), UNESCO Tokten Award (1986), Goyal Prize (1998), National Fellow of the Indian Institute of Advanced Study (2001), and Distinguished Alumnus of IIT Delhi (2002).