



ELSEVIER

Information Sciences 128 (2000) 149–154

INFORMATION  
SCIENCES

AN INTERNATIONAL JOURNAL

[www.elsevier.com/locate/ins](http://www.elsevier.com/locate/ins)

# Rotating a qubit

Subhash Kak

*Department of Electrical & Computer Engineering, Louisiana State University,  
Baton Rouge, LA 70803-5901, USA*

Received 8 October 1999; accepted 4 July 2000

---

## Abstract

Current quantum computing models implicitly assume that there is no unknown relative phase between the components of the quantum state. Arguing that this is unrealistic because of time-evolution and decoherence, we ask the question if useful computations can be performed in the presence of unknown relative phase. Specifically, we examine the problem of rotation of a qubit and examine its broader implications for quantum computing. We show that unknown phase can make it impossible to perform useful computations. © 2000 Elsevier Science Inc. All rights reserved.

---

## 1. Introduction

Quantum mechanics provides us a means of extracting information about a physical system, but this information depends on the manner in which the system is prepared and the measurement apparatus deployed. The state function of the system is defined on the complex plane whereas the observations can only be real, which means that the state function cannot be completely known. Quantum reality has been characterized as being “veiled” [3] with an underlying “implicate” order [2]. If that be the case, how can one hope to characterize this reality with such precision so as to carry out a specific computation using a single quantum state?

---

*E-mail address:* [kak@ee.lsu.edu](mailto:kak@ee.lsu.edu) (S. Kak).

Quantum computing algorithms as visualized now [7,11] proceed with the register in a pure state. Normally, this state is taken to be the all-zero state of  $n$ -qubits:  $|0\rangle|0\rangle\cdots|0\rangle$ , or the amplitude vector  $(1, 0, 0, \dots, 0)$ , which, by a process of rotation transformations on each qubit, is transformed into the state with amplitudes  $(1/\sqrt{N}, 1/\sqrt{N}, 1/\sqrt{N}, \dots, 1/\sqrt{N})$ , where  $N = 2^n$ . It is implicitly assumed that the phase uncertainty in each of these states is identical, and so it can be ignored. Is it a circumvention of the “veiling” of reality to take the components of the quantum state to be in “synchrony”? Is this assumption realistic?

There are other difficulties in predicting the evolution of the quantum state. The interaction with the environment may slow down or even freeze the dynamics of the system [1] in unexpected ways. The assembling of the system to be in the starting state will bring in further complications.

This problem was considered in a recent paper [9], where its implications for initializing the state of a quantum register were considered. We now ask specific questions: Can the cost and realizability of the initial pure state and its rotations to the superposition state be estimated? Can the evolution of the qubits be controlled?

## **2. The cost of preparing a pure state**

A pure state is one which yields a specific outcome in a given test designed to elicit the maximum number of outcomes associated with the system [10]. Examples are Stern–Gerlach experiment for spin or the use of a calcite crystal for photon polarization. One may represent the all-zero state by  $(1, 0, 0, \dots, 0)$ , if it is assumed that each of the qubits has been prepared identically and there is no dynamical evolution. This is equivalent to considering that qubits emerging out of the state preparation apparatus are frozen in their state and installed at the appropriate locations in the quantum register.

If the particles are generated at a certain point, tested to yield a specific outcome and, if they pass the test, transported to the right locations on the register, there is no way to guarantee that each of the particles would not have suffered dynamic evolution prior to installation. If instead,  $n$  tests are performed simultaneously on the particles so as to cut down on the delay, it may happen that some of these tests do not yield the specified outcome and so the failed tests will have to be repeated resulting in delay.

It is more reasonable to assume that the qubits are already available at the cell-sites of the quantum register. These qubits then will be individually steered to a specific pure state.

Note that a dynamically evolving pure state remains a pure state, since pure states are analogous to unit vectors along a set of orthogonal basis vectors, and any vector in the  $N$ -dimensional space can be taken to be one of the basis

vectors. From an information-theoretic point of view, a transition from the initial  $(1, 0, 0, \dots, 0)$  state to the  $(1, 1, 1, \dots, 1)$  superposition state is equivalent to a transition to some other  $(z_1, z_2, \dots, z_N)$  state (where  $z_i$ s are arbitrary complex numbers and it is assumed that the amplitudes are to be normalized), because each of the final states will be obtained by the application of a suitable unitary transformation. To assume that the latter state, with the unknown  $z$  weights, is *more* “complex” in some fundamental way is clearly in error. Why the superposition state  $(1, 1, 1, \dots, 1)$  “appears” to be more “basic” is because it can be obtained mathematically by the use of elegant rotation transformations on the individual qubits [7,11].

The  $n$ -qubit vector is a tensor product of the  $n$  individual qubit vectors. We assume that the qubit has somehow been steered into the appropriate superposition. As there is no reason to assume that the relative phase between the superposed component states is zero, the individual qubit at the  $i$ th location should be written as  $z_{i1}|0\rangle + z_{i2}|1\rangle$ . The  $n$ -qubit state will then have  $N - 1$  unknown relative phases and one global unknown phase.

It is common to ignore the relative phases in state vectors for ensembles, because in repeated measurements the unknown phases can be assumed to average out to zero. However, in quantum computing we speak about individual quantum systems and so this averaging out is not permissible.

In entangled states the phases do have definite relationships. But the qubits that go into the formation of the  $n$ -qubit state vector cannot be permitted to be entangled amongst themselves because current quantum algorithms do not allow it.

### 3. Preparing a qubit

For simplicity, we consider a qubit to have the form  $|\phi\rangle = \alpha e^{i\theta_1}|0\rangle + \beta e^{i\theta_2}|1\rangle$ , where  $\alpha, \beta \in R$  and  $\alpha^2 + \beta^2 = 1$ . A qubit may be prepared by starting with an available component or superposition state and transforming it into the desired superposition state by applying a unitary transformation.

The simplest way to prepare a pure state is to subject qubits to a test and discard all the qubits that do not yield the desired outcome. But we have argued why it is more reasonable to assume that the qubit is located in a given site and it is then steered to an appropriate state. Pure states are unit vectors along a set of orthogonal axes, and two examples are  $e^{i\theta_1}|0\rangle$  or  $e^{i\theta_2}|1\rangle$  at angles of  $0^\circ$  or  $90^\circ$ ; other orthogonal axes can likewise be chosen. The standard basis observables are  $|0\rangle$  and  $|1\rangle$ .

To consider different ways of initializing qubits, assume that the starting pure state is  $|0\rangle$ , determined excepting an arbitrary phase angle. One can obtain a superposition state by use of a rotation operator which, in its most general form, is the following matrix:

$$\begin{bmatrix} \alpha e^{i\theta_1} & \beta e^{-i\theta_2} \\ \beta e^{i\theta_2} & -\alpha e^{-i\theta_1} \end{bmatrix}, \quad (1)$$

where  $\theta_1$  and  $\theta_2$  are unknown phase angles. This leads to the superposition state

$$\alpha e^{i\theta_1} |0\rangle + \beta e^{i\theta_2} |1\rangle. \quad (2)$$

Here we ignore the fact that the initial state will have some uncertainty associated with it due to the impossibility of a perfect implementation of the angle of the basis vector. Furthermore, the presence of noise and entanglement with the environment imply that the superposition state will not be completely controllable, and these questions are also ignored here. If it can be arranged that  $\theta_1 = \theta_2$ , then any appropriate rotation can be achieved. But we have no means of ensuring this equality, excepting by the use of entanglement which would defeat our purpose.

If we rely on the simpler method of starting with a pure state as a unit vector in the  $45^\circ$  direction, such a pure state, when viewed from the axes at  $0^\circ$  and  $90^\circ$ , will be defined as

$$\frac{1}{\sqrt{2}}(e^{i\theta_1} |0\rangle + e^{i\theta_2} |1\rangle). \quad (3)$$

This pure state will resolve into the basis states in the directions of  $0^\circ$  and  $90^\circ$  with equal probability.

Is there a way to rotate a qubit by any specific angle? For convenience assume that the operator

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (4)$$

is implementable. When applied to the qubit  $(1/\sqrt{2})(|0\rangle + |1\rangle)$ , it will lead to the pure state  $|0\rangle$ . But since the qubit should be realistically seen to be  $(1/\sqrt{2})(e^{i\theta_1} |0\rangle + e^{i\theta_2} |1\rangle)$ , an operation by  $M$  will take the qubit only to

$$\frac{(e^{i\theta_1} + e^{i\theta_2})}{2} |0\rangle + \frac{(e^{i\theta_1} - e^{i\theta_2})}{2} |1\rangle. \quad (5)$$

The probability of obtaining a  $|0\rangle$  will now be  $(1/2)[1 + \cos(\theta_1 - \theta_2)]$ , whereas the probability of obtaining a  $|1\rangle$  will be  $(1/2)[1 - \cos(\theta_1 - \theta_2)]$ . The probabilities for the basis observables are not exactly  $1/2$ , and they depend on the starting *unknown*  $\theta$  values. Thus, the qubit can end up anywhere on the unit circle. As example, consider  $\theta_2 = 0$ ,  $\theta_1 = \pi/2$ , the probabilities of  $|0\rangle$  and  $|1\rangle$  will remain  $1/2$  even after the unitary transformation has been applied!

If one assumes that  $\theta_1 - \theta_2 = \theta_d$  is uniformly distributed over  $0$  to  $\pi$ , the probability of obtaining  $|0\rangle$  turns out to be  $1/\pi\sqrt{y - y^2}$ , where  $y$  ranges from  $0$  to  $1$ . The expected value of this continues to be  $1/2$ .

If we consider the rotation of qubit (2) by the unitary operator (4), we get the following probabilities

$$\left(\frac{1}{2}\right)[1 + \alpha\beta \cos(\theta_1 - \theta_2)], \quad \left(\frac{1}{2}\right)[1 - \alpha\beta \cos(\theta_1 - \theta_2)],$$

for obtaining the states  $|0\rangle$  and  $|1\rangle$  respectively. In other words, the fundamental phase uncertainty makes it impossible to calibrate rotation operators. Operator (4) is unable to rotate the pure state (3) by  $45^\circ$ .

Since the rotation of qubits is visualized to be done in stages in the currently conceived implementation schemes, any of these gates can introduce phase uncertainty that will be impossible to compensate for in the ongoing unitary operations.

#### 4. Conclusions

The power of the currently envisaged quantum algorithms flows from the mathematical framework of superpositions and unitary evolution [4–6,8]. But can this mathematical capacity be joined to physical reality?

Rotation operations are basic for the implementation of the currently envisaged quantum algorithms. Lacking information regarding phase of the qubit, it is clear that these operators will not work correctly. Furthermore, each gate will introduce its own random phase uncertainty because the operation  $A|\phi\rangle$  and  $Ae^{i\theta}|\phi\rangle$  are indistinguishable. As example of this, consider the unitary operator

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

which has been proposed to make the relative phases of  $|0\rangle$  and  $|1\rangle$  flip. Even assuming that the original qubit was  $(e^{i\theta}/\sqrt{2})(|0\rangle + |1\rangle)$ , the new phases become  $\theta$  and  $\theta + \pi$ , which cannot be characterized phase reversal. Since the initial phases have uncertainty, one cannot steer the qubit to a desired change.

Error correcting codes cannot be used to correct this uncertainty because it is without bound. Furthermore, if error correction worked for this problem that would allow for us to make the relative phases zero, which gets us more than what quantum theory allows.

On the other hand, if the initial phase uncertainty can be lumped together then an appropriate sequence of unitary transformations will, in principle, steer the state to the desired solution. The challenge then will be the physical implementation of this transformation in a manner so that this lumped uncertainty does not diffuse to the constituent qubits in an uncontrolled way. But even if this could be done, does the lumping together of the phase uncertainty

imply limitations with respect to implementation that will drastically reduce the advantages of quantum computers?

We conclude by raising a philosophical question: Is phase accessible to consciousness, and is this that permits the mind's control of physical processes in the brain? If the answer to this question is "yes", then it may offer understanding regarding the powers of consciousness.

## **Acknowledgements**

I am grateful to Dan Ventura for his comments on an earlier version of the paper.

## **References**

- [1] Ph. Blanchard, et al. (Eds.), *Decoherence: Theoretical, Experimental, and Conceptual Problems*, Springer, Berlin, 2000.
- [2] D. Bohm, *Wholeness and the Implicate Order*, Routledge & Kegan Paul, London, 1980.
- [3] B. d'Espagnat, *Veiled Reality: An Analysis of Present-Day Quantum Mechanical Concepts*, Addison-Wesley, Reading, MA, 1995.
- [4] D. Deutsch, Quantum computational networks, *Proc. R. Soc. Lond. A* 425 (1989) 73.
- [5] D.P. DiVincenzo, Two-bit gates are universal for quantum computation, *Phys. Rev. A* 51 (1995) 1015.
- [6] A. Ekert, R. Jozsa, Quantum computation and Shor's factoring algorithm, *Rev. Modern Phys.* 68 (1996) 733.
- [7] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.* 79 (1997) 325.
- [8] S. Kak, Quantum information in a distributed apparatus, *Foundations Phys.* 28 (1998) 1005.
- [9] S. Kak, The initialization problem in quantum computing, *Foundations Phys.* 29 (1999) 267.
- [10] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, Dordrecht, 1995.
- [11] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* 26 (1997) 1474.