The Quantum Computing (QC), Quantum Information (QI), and Quantum Encryption (QE) Curriculum. (Why? Now? Never?)

Ronald I. Frank[1]
IS Department, Pace University
Pleasantville, NY 10570 USA

Abstract

The curriculum needs for quantum computing (QC), quantum information (QI), and quantum encryption (QE) are discussed. QC is an application of Quantum Mechanics (Messiah 1958) to the problem of defining a computer using quantum phenomena. QI is an expansion of quantum mechanics analogous to classical information theory, and QE is an application of QI.

Now that the first venture capital activity in QC (Maney 2003) has occurred, it is time to start considering where, if at all, the interrelated topics QC, QI and QE belong in the Information Systems (IS) curriculum. It is argued that the topics are neither premature nor mature, so that at present they should be inserted only as descriptive topics in a hardware course and a telecommunications course. Although they will probably never be a fitting topic for a full IS course, they already are part of our culture. Soon they may come out of the research labs and begin to affect the business world.

There will always be the problem of how to effectively introduce QC and QI ideas in a "layperson's" overview. I first review the prerequisite knowledge needed to study basic QC and QI as outlined in Nielson (2000). I analogize this to four problems in covering the IS effects of some current similar highly technical topics. Second, I point out the historical parallel to the original introduction of quantum mechanics itself and relativity into society. Third, I mention a recent attempt to make QC, QI, and QE accessible to general undergraduate math students. Fourth, I discuss the alternatives, why we should bother, and I give a five-step action plan. I include an outline of four lay introductions to these topics that can be used in the action plan. Finally, I summarize and conclude that now is the time to introduce a descriptive QC topic into a hardware course and a descriptive QE topic into a telecom course.

There is no mention of QC, QI, or QE in the 2002 IS Model Curriculum (Gorgone 2002).

Keywords: quantum computing, QC, quantum information, QI, quantum encryption, QE

1. INTRODUCTION

Much research is ongoing into both the basic science and the engineering construction of a quantum computer. Also, basic science is providing mechanisms for quantum encryption QE using results from the study of quantum information. Although the QC efforts are far from a working computer, the QE efforts are further along (Singh 2002) and (eetimes 2002).

[1] rfrank@pace.edu

The intellectual prerequisites for understanding these research results and applications are quite large (Nielson 2000). They are large enough that we would not expect these topics to be part of the IS curriculum any time soon. However, just as the number theory basis for a public key infrastructure is NOT described in telecommunications books (Panko 2003), so might we expect to provide a lay perspective on QC and QI without the deeper details. Our goal for our students is cultural literacy for effective use of the technology, not effective participation in either the research or engineering.

Now that the first venture capital activity in QC (Maney 2003) has occurred, it is time to begin to consider where, if at all, the set of topics (QC, QI, and QE) belongs in the IS curriculum. I argue that the topics are neither premature nor mature, so that at present they should be included as descriptive topics: QC in a hardware course and QE in a telecommunications course. In IS, we can neglect QI for now as we neglect classical information theory. Although they will probably never be a fitting topic for a full IS course, QC and QE are presently part of our culture. Someday soon, they may come out of the research labs and begin to affect the business world.

I first review the prerequisite knowledge needed to study basic QC and QI as outlined in (Nielson 2000). I review four comparable highly technical topics not covered in IS but whose effects and high-level functionality are covered.

Second, I point out the historical parallelism between our problem and the problem society once had when introducing both relativity and quantum mechanics to the public of potential participants, supporters and users.

Third, I point out the latest attempt by the mathematics community to prepare their undergraduates in these "out of field" topics.

Fourth, I discuss our alternatives for curricula which handle QC/QI, why we should bother about it, and what we should do now. I review four available "layperson's" introductions to the ideas of QC to get the measure of the effort to introduce the ideas into the IS curriculum.

Fifth, I draw a conclusion. NOTE: there is no mention of QC, QI, or QE in the 2002 IS Model Curriculum (Gorgone 2002).

2. QC/QI INTELLECTUAL PREREQUISITES

To quote from the preface of one of the most widely used and referenced textbooks in the subject (Nielson 2000): "Our purpose in this book is therefore twofold. First, we introduce the background material in computer science, mathematics, and physics necessary to understand Quantum Computation and Quantum Information. This is done at a level comprehensible to readers with a background at least the equal of a beginning graduate student in one or more of these three disciplines; …"

The computer science they refer to is hardcore complexity theory, basic circuit theory and technology, automata theory, and algorithm analysis. The mathematics (which they say also requires "mathematical maturity") includes advanced linear algebra (hermitian and unitary operators on finite and infinite dimensional vector spaces (elementary Hilbert space theory), Fourier transforms, and elementary group theory. The physics prerequisite includes familiarity with classical mechanics, and the basic ideas in electromagnetic theory.

This is not the background of the typical undergraduate or graduate IS student. So, does this mean that there is no role here for QC/QI/QE in the IS curriculum? No. Our problem to find a way to provide a user's or layperson's introduction to these topics.

Analogies to Other Technical Topics

How do we handle other highly technical topics in the IS curriculum? Let us examine some analogous examples from one popular book: Panko (Panko 2003):

1) Information theory behind the concept of bandwidth: he does quote the "Shannon Equation" on page 88, but provides only a brief discussion without any derivations.

2) The concept of channel in communications: he defines a channel as a band of frequencies on page 87 but there is no discussion of the Shannon information theory results covering noiseless and noisy channels.
3) Number theory behind Public Key Infrastructure (PKI): he asserts the existence of public key - private key pairs and explains their use (including message digests for digital signatures on pg. 302) but there is no discussion of the number theory deriving their values and properties.

I have seen other books in this area that did discuss in outline the ideas behind PKI, "information" and "noise," but they did present learning problems for the typical IS student. I call Panko's approach the descriptive approach, in which one describes the functionality but not its basis in science. This is the approach we will need for QC/QI/QE.

Another example is more controversial. Again, from popular books (Hoffer 2002), (Pressman 2001), and (Whitten 2004):

4) Consider the current state of cost estimation in software development. The ascendant COCOMO II (Boehm 2000) and its derivatives require the manipulation of exponentials and the use of at least a calculator with X^Y for classroom and homework examples. It also requires an understanding (at least in principle) of how nonlinear parameter estimation can be used to summarize historical data to arrive at the exponential models (also why there are correction "fudge" factors).

The IS book by Hoffer et al, (Hoffer 2002) does not go into cost estimation and a fortiori does not mention the COCOMO II models. The CS book by Pressman (Pressman 2001) does mention cost estimating and the simplified COCOMO I but he considers COCOMO II beyond the scope of the book (pg. 133) even though it is the preeminent costing technique now used by larger organizations. Whitten et al, (Whitten 2004) also does not cover COCOMO.

I consider these to be clear examples of where IS is letting our students down by its flight from mathematics and rigor. Are we about to do the same with QC/QI/QE?

3. HISTORICAL PARALLELISM

In 1905, it was said that only 5 men understood special relativity, but by 1955, this topic was being taught in second semester freshman college physics courses, both for physics majors and for pre-med students. Now it appears in high school advanced placement courses because the prerequisites were reduced to only high school physics and algebra.

In 1925-28 the new (i.e. the present) quantum theory was proposed by Heisenberg, (matrix mechanics), and Schroedinger, Born, Jordon, and De Broglie (wave mechanics). It required mathematical knowledge that was only first organized into a book the year before (1924). This book (in German) was the Methods of Mathematical Physics by Courant and Hilbert (Courant 1953). This may be the first example of Just-Before-Time (prescient) publishing. Courant wrote it, using notes from Hilbert's lectures.

Courant's motivation was to provide a text book for both mathematics students and students of physics that organized the new mathematics. The entire first volume is "nothing but" the generalization of the solution of algebraic equations. Courant proceeds from the 8^{th} grade solution of simultaneous equations to matrices to linear transformations to eigenvalue problems (wave equations) to expansion of functions in orthogonal sets of eigenfunctions (arbitrary system state in terms of e.g., energy eigenfunctions). All of this is done in only the first 20% of the book (111 pages).

A later section on Sturm-Liouville problems covers the mathematics of basic quantum mechanical one dimensional systems. Courant actually discusses the Schroedinger equation eigenvalue problem (this is inserted into later editions).

We need an IS Courant-Hilbert for the layperson for QC/QI/QE.

4. A MATHEMATICIAN'S ATTEMPT AT BACKGROUNDING MATH STUDENTS

The mathematics community is beginning to prepare introductory material on these topics for their students. (Gudder 2003) is a 21 page introduction that assumes "only a basic knowledge of linear algebra." He uses among other linear algebra topics, inner products on tensor product spaces (multilinear algebra). He talks about quantum coding (encoding not programming) and teleportation. He introduces quantum circuits and quantum Fourier transforms. I would say he also requires the usual knowledge of AND, OR, NOT of logic circuits and some previous exposure to the Fourier transform, although not an actual computational facility with them.

5. OUR ALTERNATIVES

We could hope the problem never arises, i.e., QC/QI/QE die on the vine. We can ignore the curriculum issue for now (the most likely scenario). We can dither ineffectually for a long time over what and when and if we should act or we can begin to take effective initial curriculum steps (in the spirit of iterative refinement).

Why Bother?

Before long we will have to address QC/QI/QE, if only because we and our students should participate in the public policy issue of funding for research in this area, which may take decades to come to market. On the other hand, Quantum Encryption has been successfully demonstrated and will probably appear in the market place in the next five years (Johnson 2002). In that case, our students should at least have a layperson's understanding of its functionality.

What To Do Now

We need five kinds of near-term efforts:

1) First, we have to inform ourselves.
2) We then need discussions on curriculum formation.
3) We need to author initial text material in article form or booklet form.
4) We need to try these out in a classroom setting.
5) Finally we will need to evaluate the effectiveness of our approach.

To begin with, I think we should add a special topic to a computer organization or computer architecture course that outlines the current state of QC. It can be based on readings from (Johnson 2003) and (Aczel 2003). Similarly, we can add a topic to the standard telecommunications course that would outline Quantum Encryption (bypassing QI completely, for now) based on the section in (Singh 2002).

These additions have to be factored into the follow-on to the 2002 IS Model Curriculum (Gorgone 2002).

Four Lay Introductions for Background

The only lay introduction to QC proper that I have found is (Johnson 2003). It includes a chapter on QE.

A more historical and specialized (but still layperson's) book is (Aczel 2003) which discusses one of the most unintuitive aspects of Quantum Mechanics, called entanglement, which is also one of the most fundamental sources of the power of QE.

There is a third, more complete, lay introduction to Quantum Physics for "popular science readers" (Treiman 1999). Unfortunately, it was written in the ancient era (1999), at the dawn of QC. This book contains no reference to QC, QI, or QE. However, it provides a very good background for the lay understanding of Quantum Mechanics.

The first two books, (Johnson 2003) and (Aczel 2003), provide more than enough material from which to choose readings which can introduce these quantum ideas into the IS curriculum. They can be the basis of a set of QC readings in a hardware course and QE readings in a telecom course. They each are relatively short books and easy reads.

A fourth book (for QE only) (Singh 2002) contains a layperson's introductory chapter on QE.

6. CONCLUSION: PROBLEM AND SOLUTION

These new technologies (QC, QI, and QE) are beyond our ken for now. However, we have to begin to prepare ourselves and the materials for our students so we can teach technologies as far as they affect IS.

The final conclusion is that we can introduce topics into the current curriculum to provide cultural literacy in these areas. See my comments about the reference (Johnson 2003) below.

We can insert a useful (QC) topic in a hardware course and a (QE) topic in a telecommunications course by the use of assigned readings. A one semester elective introductory course on QC/QI/QE is possible only if we upgrade the mathematical prerequisites in IS to include a basic linear algebra background. See sections 3 and 4 above.

In deed, perhaps we should move toward a general requirement that IS students take an introductory course in linear algebra. This too is not in the 2002 Model Curriculum (Gorgone 2002).

7. REFERENCES

Aczel, Amir D. 2001, Entanglement. Four Walls Eight Windows Pubs. ISBN: 1-56858-232-3.

{Layperson's introduction to quantum entanglement.}

Boehm, Barry, 2000, Software Cost Estimation With COCOMO II. Prentice Hall ISBN: 0-13-026692-2.

{Updated documentation on the massive practical research project at USC that has led to some of the most widely used software project costing and estimating methodologies and products.}

Courant, Richard, David Hilbert, 1953, Methods of Mathematical Physics Volume I. 5th English Ed. John Wiley & Sons; (1989) ISBN:: 0471557609.

{Seminal textbook source of the basic mathematical foundations of quantum mechanics. One of the historical greats.}

Gorgone, John T., Gordon B. Davis, Joseph S. Valacich, Heikki Topi, David L. Feinstein, Herbert E. Longenecker, Jr., "IS 2002 Model Curriculum and Guidelines for Undergraduate Degree Programs in Information Systems." (2002). Association for Information Systems. http://192.245.222.212:8009/IS2002Doc/

{No reference to QC, QI, or QE is contained in this document.}

Gudder, Stan "Quantum Computation." The American Mathematical Monthly March 2003 # 110 pp. 181 – 201.

{Intro to QC for the mathematically prepared under grad.}

Hoffer, Jeffrey, Joey George, and Joseph Valacich, 2002, Modern Systems Analysis & Design. 3rd Ed. Prentice Hall ISBN: 0-13-033990-3.

{Standard IS systems analysis and design textbook.}

Johnson, R. Colin "Hackers beware: quantum encryption is coming" November 12, 2002 http://www.eetimes.com/at/news/OEG20021111S0036.

{An article about QE success and imminence.}

Johnson, George, 2003, A Short Cut Through Time. Alfred A. Knoph Pubs. ISBN: 0-375-41193-3.

{Layperson's introduction to QC and QE. My choice for selected topic readings in IS courses – see the conclusions section 6 above.}

Maney, Kevin, "Quantum computing is out there, and it just got funding" http://www.usatoday.com /usatonline/20030625 //5271878s.htm (June 25, 2003).

{Announces a venture capital effort to build a quantum computer.}

Messiah, Albert, 1958, Quantum Mechanics. Dover (1999 paper version of the John Wiley 1958 two volume set) ISBN: 0-486-40924-4.

{I include this reference only for completeness, not as a suggested starting point. It is an old favorite of mine, is readily available, complete, and inexpensive. It is not an IS book. It is a well-known text for graduate work in physics and assumes a substantial background in both physics and mathematics such as a large part of (Courant 1953).

It contains no information on the modern topics of QC, QI, or QE, having come before these, but it is a pleasant read for a deeper background.}

Nielson, Michael A. and Isaac L. Chuang, 2000, Quantum Computation and Quantum Information. Cambridge University Press ISBN: 0-52163503-9.

{Possibly the most widely referenced textbook in QC, QI, and QE (cryptography here.)}

Panko, Raymond R., 2003, Business Data Networks and Telecommunications. 4th Ed. Prentice Hall ISBN: 0-13-035914-9.

{Standard IS telecommunications textbook.}

Pressman, Rodger, 2001, Software Engineering. 5th Ed. McGraw-Hill ISBN: 0-07-365578-3.

{Standard CS software engineering textbook.}

Singh, Simon, 2002, The Code Book. Anchor Books ISBN: 0-385-49532-3.

{Includes a layperson's chapter on modern QE.}

Treiman, Sam, 1999, The Odd Quantum. Princeton University Press, ISBN: 0-691-00926-0.

{Layperson's introduction to quantum mechanics.}

Whitten, Jeffrey, Lonnie Bentley, and Kevin Dittman, 2004, Systems Analysis and Design Methods. 6th Ed. McGraw Hill – Irwin ISBN: 0-07-247417-3.

{Standard IS systems analysis and design textbook.}