A CONTINUOUS VARIABLE SHOR ALGORITHM

SAMUEL J. LOMONACO, JR. AND LOUIS H. KAUFFMAN

Abstract. In this paper, we use the methods found in [12] to create a continuous variable analogue of Shor's quantum factoring algorithm. By this we mean a quantum hidden subgroup algorithm that finds the period P of a function

$$\Phi : \mathbb{R} \longrightarrow \mathbb{C}$$

from the reals $\mathbb{R}$ to the complex numbers $\mathbb{C}$, where Φ belongs to a very general class of functions, called the class of admissible functions. This algorithm gives some insight into the inner workings of Shor's quantum factoring algorithm. Whether or not it can be implemented remains to be determined.

Contents

Date: September 25, 2002.

1991 *Mathematics Subject Classification.* [2000]Primary 81P68; Secondary 68Q05, 81Q99.

Key words and phrases. Quantum algorithms, continuous variable, Shor's algorithm, generalized functions, distributions, rigged Hilbert spaces, Gelfand triplets.

This effort is partially supported by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory, Air Force Materiel Command, USAF, under agreement number F30602-01-2-0522, the National Institute for Standards and Technology (NIST), and by L-O-O-P Fund Grant BECA2002. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright annotations thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Defense Advanced Research Projects Agency, the Air Force Research Laboratory, or the U.S. Government. The first author gratefully acknowledges the hospitality of the Mathematical Science Research Institute , Berkeley, California, where some of this work was completed, and would also like to thank Howard Brandt and Dan Gottesman for some helpful conversations.

1. Introduction

In this paper, we create a continuous variable analogue of Shor's quantum factoring algorithm. This algorithm is called a continuous variable Shor algorithm for the following reason. Recall that Shor's quantum factoring algorithm [18], [17], [13] reduces the task of factoring an integer N to that of finding the period P of a function

$$\Phi : \mathbb{Z} \longrightarrow \mathbb{Z} \operatorname{mod} N$$

from the integers $\mathbb{Z}$ to the integers $\mathbb{Z}$ modulo N. So by a continuous variable analogue to Shor's factoring algorithm, we mean a quantum algorithm that finds the period P of a function

$$\Phi : \mathbb{R} \longrightarrow \mathbb{C}$$

from the reals $\mathbb{R}$ to the complex numbers $\mathbb{C}$.

This quantum algorithm sheds some light on the inner workings of Shor's factoring algorithm. Whether or not it is implementable remains to be determined.

Continuous variable algorithms for two other quantum algorithms are to be found in the open literature. A continuous variable analogue of Grover's algorithm was constructed by Pati, Braustein, and Lloyd in [2]; and a continuous variable Deutsch-Jozsa algorithm was recently created by Pati and Braustein in [3].

2. Mathematical machinery

To create a continuous variable analogue of Shor's algorithm, we will need to make use of the mathematical machinery of **generalized functions** (also known as **distributions**) and of **rigged Hilbert spaces** (also known as **Gelfand triplets**.) For a more in depth discussions of this mathematical machinery, we refer the reader to [1], [6], [7], [8], [15], and [16].

2.1. Generalized functions.

In regard to generalized functions, the reader is no doubt familiar with one generalized function, namely, the Dirac delta function

$$\delta\left(x\right)$$

on the reals $\mathbb{R}$. We will also make use of the following generalized function

$$\delta_P\left(x\right) = \frac{1}{\left|P\right|} \sum_{n=-\infty}^{\infty} \delta\left(x - \frac{n}{P}\right) ,$$

which is an infinite sum of Dirac delta functions over the lattice $\left\{\frac{n}{P} : n \in \mathbb{Z}\right\}$, where P is a nonzero real number.

2.2. **Rigged Hilbert spaces.** We will make use of a number of rigged Hilbert spaces. The first is the rigged Hilbert space $\mathcal{H}_{\mathbb{R}}$ with **orthonormal basis**

$$\{|x\rangle : x \in \mathbb{R}\} ,$$

where by **orthonormal** we mean there is a bracket product on $\mathcal{H}_{\mathbb{R}}$ defined by

$$\langle x \mid y \rangle = \delta (x - y) \ \ .$$

The elements of $\mathcal{H}_{\mathbb{R}}$ are formal integrals of the form

$$\int_{-\infty}^{\infty} dx \ f(x) |x\rangle \ \ ,$$

where $f : \mathbb{R} \longrightarrow \mathbb{C}$ is a function or a generalized function.

For x_0 a constant, we define

$$|x_0\rangle = \int\limits_{-\infty}^{\infty} dx \ \delta (x - x_0) |x\rangle$$

Since the Dirac delta function is a tempered distribution [15], it follows that

$$\langle y_0 \mid x_0 \rangle = \begin{cases} 1 & \text{if } x_0 = y_0 \\ \\ 0 & \text{otherwise} \end{cases}$$

The second is the rigged Hilbert space $\mathcal{H}_{\mathbb{C}}$ with orthonormal basis

$$\{|y\rangle : y \in \mathbb{C}\} .$$

Finally, we will also need the tensor product rigged Hilbert space $\mathcal{H}_{\mathbb{R}} \otimes \mathcal{H}_{\mathbb{C}}$ with orthonormal basis

$$\{|x\rangle |y\rangle : x \in \mathbb{R} \text{ and } y \in \mathbb{C}\} .$$

3. Fourier analysis on the real line $\mathbb{R}$

Let $\Phi : \mathbb{R} \longrightarrow \mathbb{C}$ be a periodic admissible function of minimum period P from the reals $\mathbb{R}$ to the complex numbers $\mathbb{C}$.

Remark 1. *We have intentionally not defined the term 'admissible,' since there are many possible definitions of this term. For example, one workable definition of an admissible function is a function that is Lebesgue integrable on every closed subinterval of the reals* $\mathbb{R}$.

We seek to define the Fourier transform of Φ. Since Φ in general is neither L^1 nor L^2 nor of compact support, the usual definitions of the Fourier transform will not apply. So we need to be a bit creative.

We proceed to define the Fourier transform as follows:

Definition 1. *Let* $\Phi : \mathbb{R} \longrightarrow \mathbb{C}$ *be a periodic admissible function of minimum period* P *from the reals* $\mathbb{R}$ *to the complex numbers* $\mathbb{C}$. *We interpret the standard expression* $\int_{-\infty}^{\infty} dx\ e^{-2\pi ixy}\Phi(x)$ *for the Fourier transform* $\widehat{\Phi} : \mathbb{R} \longrightarrow \mathbb{C}$ *as the generalized function*

$$\widehat{\Phi}(y) = \delta_P(y) \int_0^P dx\ e^{-2\pi ixy}\Phi(x)$$

where

$$\delta_P(y) = \frac{1}{|P|} \sum_{n=-\infty}^{\infty} \delta\left(y - \frac{n}{P}\right) \ .$$

Remark 2. *The above definition can be motivated as follows:*

$$\begin{aligned}
\int_{-\infty}^{\infty} dx\ e^{-2\pi ixy}\Phi(x) &= \sum_{n=-\infty}^{\infty} \int_{nP}^{(n+1)P} dx\ e^{-2\pi ixy}\Phi(x) \\
&= \sum_{n=-\infty}^{\infty} \int_0^P dx\ e^{-2\pi i(x+nP)y}\Phi(x+nP) \\
&= \sum_{n=-\infty}^{\infty} e^{-2\pi inPy} \int_0^P dx\ e^{-2\pi ixy}\Phi(x) \\
&= \sum_{n=-\infty}^{\infty} \tfrac{1}{|P|}\delta\left(y - \tfrac{n}{P}\right) \int_0^P dx\ e^{-2\pi ixy}\Phi(x) \\
&= \delta_P(y) \int_0^P dx\ e^{-2\pi ixy}\Phi(x)
\end{aligned}$$

where, in the context of distributions, we have

$$\sum_{n=-\infty}^{\infty} e^{-2\pi inPy} = \frac{1}{|P|}\delta\left(y - \frac{m}{P}\right) \ , \text{ for } y \in \left[\frac{m}{P}, \frac{m+1}{P}\right)$$

(See [15].*)*

The reader can easily verify that the inverse Fourier transform behaves as expected, i.e., that

Proposition 1.

$$\Phi(x) = \int_{-\infty}^{\infty} dy\ e^{-2\pi ixy}\widehat{\Phi}(y)$$

4. The algorithm for finding integer periods

Let
$$\Phi : \mathbb{R} \longrightarrow \mathbb{C}$$
be a periodic admissible function of minimum period P from the reals $\mathbb{R}$ to the complex numbers $\mathbb{C}$. We will now create a continuous variable Shor algorithm to find integer periods. In later sections, we will extend the algorithm to rational periods, and then to irrational periods.

We construct two quantum registers
$$|\text{Left Register}\rangle \text{ and } |\text{Right Register}\rangle$$
called left- and right-registers respectively, and 'living' respectively in the rigged Hilbert spaces $\mathcal{H}_{\mathbb{R}}$ and $\mathcal{H}_{\mathbb{C}}$. The left register was constructed to hold arguments of the function Φ, the right to hold the corresponding function values.

We assume we are given the unitary transformation
$$U_\Phi : \mathcal{H}_{\mathbb{R}} \otimes \mathcal{H}_{\mathbb{C}} \longrightarrow \mathcal{H}_{\mathbb{R}} \otimes \mathcal{H}_{\mathbb{C}}$$
defined by
$$U_\Phi : |x\rangle\,|y\rangle \longmapsto |x\rangle\,|y + \Phi(x)\rangle$$

Finally, we choose a large positive integer Q, so large that $Q \geq 2P^2$.

The quantum part of our algorithm consists of **Step 0** through **Step 4** as described below:

Step 0 Initialize
$$|\psi_0\rangle = |0\rangle\,|0\rangle$$

Step 1 Apply the inverse Fourier transform to the left register, i.e. apply $\mathcal{F}^{-1} \otimes 1$ to obtain
$$|\psi_1\rangle = \int_{-\infty}^{\infty} dx\ e^{2\pi i x \cdot 0}\,|x\rangle\,|0\rangle = \int_{-\infty}^{\infty} dx\ \ |x\rangle\,|0\rangle$$

Step 2 Apply $U_\Phi : |x\rangle\,|u\rangle \longmapsto |x\rangle\,|u + \Phi(x)\rangle$ to obtain
$$|\psi_2\rangle = \int_{-\infty}^{\infty} dx\ \ |x\rangle\,|\Phi(x)\rangle$$

Step 3 Apply the Fourier transform to the left register, i.e. apply $\mathcal{F} \otimes 1$ to obtain

$$
\begin{aligned}
|\psi_3\rangle &= \int_{-\infty}^{\infty} dy \int_{-\infty}^{\infty} dx \; e^{-2\pi i x y} \, |y\rangle \, |\Phi(x)\rangle \\
&= \int_{-\infty}^{\infty} dy \;\; |y\rangle \, \delta_P(y) \int_{0}^{P-} dx \; e^{-2\pi i x y} \, |\Phi(x)\rangle \\
&= \sum_{n=-\infty}^{\infty} \left| \frac{n}{P} \right\rangle \left(\frac{1}{|P|} \int_{0}^{P-} dx \; e^{-2\pi i x \frac{n}{P}} \, |\Phi(x)\rangle \right) \\
&= \sum_{n=-\infty}^{\infty} \left| \frac{n}{P} \right\rangle \left| \Omega\left(\frac{n}{P} \right) \right\rangle
\end{aligned}
$$

where

$$
\left| \Omega\left(\frac{n}{P} \right) \right\rangle = \frac{1}{|P|} \int_{0}^{P-} dx \; e^{-2\pi i x \frac{n}{P}} \, |\Phi(x)\rangle \;\; ,
$$

and where $\int_{0}^{P-} dx \, e^{-2\pi i x \frac{n}{P}} \, |\Phi(x)\rangle$ denotes the formal integral $\int_{0}^{P} dx \, e^{-2\pi i x \frac{n}{P}} \left[1 - \delta(x - P) \right] |\Phi(x)\rangle$.

Step 4 Measure the left register with respect to the observable

$$
\mathcal{O} = \int_{-\infty}^{\infty} dy \; \frac{\lfloor Qy \rfloor}{Q} \, |y\rangle \, \langle y|
$$

to produce a random eigenvalue

$$
\frac{m}{Q} \; ,
$$

where $\lfloor Qy \rfloor$ denotes the greatest integer $\leq Qy$, and then determine whether $\frac{m}{Q}$ can be used to find the period P.

5. The observable $\mathcal{O}$

In this section, we now discuss the above **Step 4** in greater detail.

The spectral decomposition of the observable $\mathcal{O}$ is given by

$$
\mathcal{O} = \int_{-\infty}^{\infty} dy \; \frac{\lfloor Qy \rfloor}{Q} \, |y\rangle \, \langle y| = \sum_{m=-\infty}^{\infty} \left(\frac{m}{Q} \right) P_m \; ,
$$

where P_m denotes the projection operator

$$P_m = \int_{\frac{m}{Q}}^{\frac{m+1}{Q}-} dy \ \left|y\right\rangle \left\langle y\right| \equiv \int_{\frac{m}{Q}}^{\frac{m+1}{Q}} dy \ \left[1 - \delta\left(y - \frac{m+1}{Q}\right)\right] \left|y\right\rangle \left\langle y\right|$$

Measurement of

$$\left|\psi_3\right\rangle = \sum_{n=-\infty}^{\infty} \left|\frac{n}{P}\right\rangle \left|\Omega\left(\frac{n}{P}\right)\right\rangle$$

will always produce an eigenvalue $\frac{m}{Q}$ for which there exists an integer n such that

$$\frac{m}{Q} \leq \frac{n}{P} < \frac{m+1}{Q}$$

We seek to determine the unknown rational $\frac{n}{P}$ from the known rational eigenvalue $\frac{m}{Q}$.

If $Q \geq 2P^2$, then the unknown rational $\frac{n}{P}$ will be a convergent of the continued fraction expansion of the known eigenvalue $\frac{m}{Q}$. Thus, the continued fraction recursion can be used to determine the period P.

6. The algorithm for finding rational periods

We now extend the above algorithm to one for finding rational periods

$$P = \frac{a}{b}, \quad \gcd(a, b) = 1$$

We choose an integer $Q \geq 2a^2$.

Part 1 *Execute the above steps* **Step 0** *through* **Step 4** *twice to produce two eigenvalues*

$$\frac{m_1}{Q} \text{ and } \frac{m_2}{Q},$$

and then goto **Part 2**.

Since $Q \geq 2a^2$, the eigenvalues $\frac{m_1}{Q}$ and $\frac{m_2}{Q}$ will have unique convergents respectively of the form

$$\frac{n_1 b}{a} \text{ and } \frac{n_{2b}}{a}$$

(See [10, Theorem 184, Section 10.15].)

If the following Condition A is satisfied, then the reciprocal period is simply given by

$$\frac{1}{P} = \frac{\gcd(n_1 b, n_2 b)}{a}$$

Condition A. $\boxed{\gcd(n_1, n_2) = 1, \ \gcd(n_1, a) = 1, \quad \gcd(n_2, a) = 1}$

If we assume that CONDITION A is satisfied, then the above expression for the reciprocal period can be computed in $\boxed{\textbf{Part 2}}$ given below:

$\boxed{\textbf{Part 2}}$ *Execute the following:*

$\boxed{\textbf{Step 5}}$ *Compute all the convergents* $\left\{\frac{p_{1k}}{q_{1k}} : k = 1, 2, \ldots, K\right\}$ *and* $\left\{\frac{p_{2\ell}}{q_{2\ell}} : \ell = 1, 2, \ldots, L\right\}$ *of* $\frac{m_1}{Q}$ *and* $\frac{m_2}{Q}$, *respectively*

$\boxed{\textbf{Step 6}}$ *Search for denominators* q_{1k} *and* $q_{2\ell}$ *which are equal*

FOR $k = 1, 2, \ldots, K$ DO
  FOR $\ell = 1, 2, \ldots, L$ DO
    IF $q_{1k} = q_{2\ell}$ THEN
      LET $q = q_{1k} = q_{2\ell}$ *and* $\alpha = \frac{q}{\gcd(p_{1k}, p_{2\ell})}$
      IF α *is a period of* Φ THEN
        OUTPUT α *and* STOP # *Period found*
  ENDFOR
ENDFOR
GOTO $\boxed{\textbf{Part 1}}$ # *Period not found*

$\boxed{\textbf{Part 2}}$ will find and output the period P provided the output of $\boxed{\textbf{Part 1}}$ satisfies CONDITION A. From the last corollary of the Appendix, we know this will occur after $\boxed{\textbf{Part 1}}$ is repeated an average of $O\left((\lg\lg a)^2\right) = O\left((\lg\lg Q)^2\right)$ times. However, since we do not know until the completion of $\boxed{\textbf{Part 2}}$ whether or not the output of $\boxed{\textbf{Part 1}}$ satisfies Condition A , both $\boxed{\textbf{Part 1}}$ and $\boxed{\textbf{Part 2}}$ need to be repeated on average at most $O\left((\lg\lg Q)^2\right)$ to finally find the output P.

Remark 3. *One can quadratically speedup* $\boxed{\textbf{\textit{Step 6}}}$ *by taking advantage of the fact that the convergent denominators are linearly ordered.*

7. Finding irrational periods

The above algorithm can be extended to finding, to any degree of desired precision, the period P of a periodic admissible function Φ when the period P is irrational. But in this case, there is a severe restrictive condition that must be imposed on the function Φ. Namely, we need to assume that the function Φ is continuous. This continuity condition is needed for determining whether or not a rational is sufficiently close to the unknown irrational period.

8. Conclusion

The continuous variable quantum algorithm constructed in this paper does give some insight into the inner workings of Shor's original quantum factoring algorithm. On the other hand, the quantum algorithm constructed in this paper raises many more questions than it answers. Can this algorithm be implemented? Can an approximation of this algorithm be implemented? Does this quantum algorithm shed some light on Hallgren's quantum algorithm [9] for solving Pell's equation?

9. Appendix. Number theoretic probabilities.

In this Appendix, we derive an asymptotic lower bound $\Omega\left(\left(\frac{1}{\lg\lg a}\right)^2\right)$ on the probability that the output of $\boxed{\textbf{Part 1}}$ of the algorithm found in Section 6 of this paper will satisfy the Condition A defined within that Section.

Notation Convention. *Throughout this section, the symbol 'p' will always be used to denote a prime integer.*

Proposition 2. *Let a be a fixed positive integer. Then for every positive integer $N \geq a$, if an integer n is randomly chosen from the set integers*

$$\{k \in \mathbb{Z} : 0 < k \leq N\}$$

according to the uniform probability distribution, then the probability $Prob_N\left(\gcd(a,n)=1\right)$ that n is relatively prime to a is bounded below by

$$Prob_N\left(\gcd(a,n)=1\right) \geq \frac{\varphi(a)}{a},$$

where $\mathbb{Z}$ denotes the set of integers, and where φ denotes the Euler phi function.

Proof.

$$Prob_N\left(\gcd(a,n)=1\right) = \prod_{p|a}\left(1-\frac{\lfloor N/p\rfloor}{N}\right) \geq \prod_{p|a}\left(1-\frac{1}{p}\right) = \frac{\varphi(a)}{a}$$

□

As a corollary, we have:

Corollary 1. *Let a be a fixed positive integer. Then for every positive integer $N \geq a$, if two n_1 and n_2 are two random integers chosen independently with replacement from the set integers*

$$\{k \in \mathbb{Z} : 0 < k \leq N\}$$

according to the uniform probability distribution, then the probability $Prob_N\left(\gcd(a,n_1)=1=\gcd(a,n_2)\right)$ that both n_1 and n_2 are relatively prime to a is bounded below by

$$Prob_N\left(\gcd(a,n_1)=1=\gcd(a,n_2)\right) \geq \left(\frac{\varphi(a)}{a}\right)^2,$$

where $\mathbb{Z}$ denotes the set of integers, and where φ denotes the Euler phi function.

Proposition 3. *Let a be a fixed positive integer. Then for every positive integer $N \geq a$, if two n_1 and n_2 are two random integers chosen independently with replacement from the set of integers*

$$\{k \in \mathbb{Z} : 0 < k \leq N\}$$

according to the uniform probability distribution, then the conditional probability

$$Prob_N \Big(\gcd(n_1, n_2) = 1 \mid \gcd(a, n_1) = 1 = \gcd(a, n_2) \Big)$$

that n_1 and n_2 are relatively prime given that n_1 and n_2 are both relatively prime to a is bounded below by

$$Prob_N \Big(\gcd(n_1, n_2) = 1 \mid \gcd(a, n_1) = 1 = \gcd(a, n_2) \Big) \geq \frac{6}{\pi^2},$$

where $\mathbb{Z}$ denotes the set of integers, and where φ denotes the Euler phi function.

Proof.

$$\begin{aligned} Prob_N \left(\gcd(n_1, n_2) = 1 \middle| \begin{array}{c} \gcd(a, n_1) = 1 \\ \text{and} \\ \gcd(a, n_2) = 1 \end{array} \right) &= \prod_{\substack{p \\ p \nmid a \text{ and } p \leq N}} \left(1 - \left(\frac{\lfloor N/p \rfloor}{N} \right)^2 \right) \\ &\geq \prod_{\substack{p \\ p \nmid a \text{ and } p \leq N}} \left(1 - p^{-2} \right) \\ &> \prod_{p} \left(1 - p^{-2} \right) = \zeta(2)^{-1} = \frac{6}{\pi^2} \end{aligned}$$

where ζ denotes the Riemann zeta function. (See [10].) $\square$

Corollary 2. *Let a be a fixed positive integer. Then for every positive integer $N \geq a$, if two n_1 and n_2 are two random integers chosen independently with replacement from the set of integers*

$$\{k \in \mathbb{Z} : 0 < k \leq N\}$$

according to the uniform probability distribution, then the probability

$$Prob_N \Big(\gcd(n_1, n_2) = \gcd(a, n_1) = \gcd(a, n_2) = 1 \Big)$$

that the integers a, n_1, n_2 are all relatively prime to each other is bounded below by

$$Prob_N \Big(\gcd(n_1, n_2) = \gcd(a, n_1) = \gcd(a, n_2) = 1 \Big) \geq \frac{6}{\pi^2} \left(\frac{\varphi(a)}{a} \right)^2,$$

where $\mathbb{Z}$ denotes the set of integers, and where φ denotes the Euler phi function. Moreover, we have the asymptotic bound

$$Prob_N \Big(\gcd(n_1, n_2) = \gcd(a, n_1) = \gcd(a, n_2) = 1 \Big) = \Omega \left(\left(\frac{1}{\lg \lg a} \right)^2 \right)$$

Proof. The first part of this corollary follows immediately from the above corollary and proposition. The second part follows immediately from a number theoretic theorem found in [10, Theorem 328, Section 18.4] which states that

$$\liminf \frac{\varphi(a)}{a/\ln\ln a} = e^{-\gamma},$$

where γ denotes Euler's constant. $\square$

10. References

References

[1] Bohm, A., **"The Rigged Hilbert Space and Quantum Mechanics,"** Springer-Verlag, (1978).

[2] Pati, Arun K., Samuel L. Braustein, and Seth Lloyd, **Quantum searching with continuous variables**, http://xxx.lanl.gov/abs/quant-ph/0002082.

[3] Pati, Arun K., and Smauel Braustein, **Deutsch-Jozsa algorithm for continuous variables**, http://xxx.lanl.gov/abs/quant-ph/0207108.

[4] Brukner, Caslav, Myungshik S. Kim, Jia-Wei Pan, and Anton Zeilinger, **Correspondence between continuous variable and discrete quantum systems of arbitrary dimensions**, http://xxx.lanl.gov/abs/quant-ph/0208116.

[5] Dirac, P.A.M., **"The Principles of Quantum Mechanics,"** Clarendon Press, (1958).

[6] Gadella, M., and F. Gomez, **A unified mathematical formalism for the Dirac formulation of quantum mechanics,** Plenum Publishing Corporation, (2002), pp. 815 - 869.

[7] Gelfand, I.M., and G.E. Shilov, **"Generalized Functions, Vol. II,"** Academic Press, (1967).

[8] Gelfand, I.M., and N.J. Vilenkin, **"Generalized Functions, Vol. IV,"** Academic Press, (1967).

[9] Hallgren, Sean, **Polynomial-Time Quantum Algorithms for Pell's Equation and the Principal Ideal Problem,** STOC 2002.

[10] Hardy, G.H., and E.M. Wright, **"An Introduction to the Theory of Numbers,"** Oxford Press, (1965).

[11] Knuth, Donald E., "**The Art of Computer Programming,"** (second edition), Addison-Wesley, Reading, Massachusetts, (1981).

[12] Lomonaco, Samuel J., Jr., and Louis H. Kauffman, **Quantum hidden subgroup problems: A mathematical perspective,** AMS CONM/305, 2002. http://xxx.lanl.gov/abs/quant-ph/0201095

[13] Lomonaco, Samuel J., Jr., **Shor's quantum factoring algorithm,** AMS PSAPM/58, (2002), pp. 161 - 179.

[14] Lomonaco, Samuel J. Lomonaco, Jr., (editor), **"Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium,"** PSAPM 58, American Mathematical Society, Providence, RI, (2002).

[15] Richards, J. Ian, and Heekyung K. Youn, **"Theory of Distributions,"** Cambridge University Press, (1990).

[16] Schwartz, L., **"Théorie des Distributions,"** vols. I et II, Herman et Cie, Paris, (1950, 1951).

[17] Shor, Peter W., **Introduction to quantum algorithms,** AMS PSAPM/58, (2002), pp. 143 - 159.

[18] Shor, P. W., **Polynomial-time algorithms for prime factorization and discrete logorithms on a quantum computer,** SIAM J. Computing, **26**, (1997), pp. 1484 - 1509.

University of Maryland Baltimore County, Baltimore, MD 21250, and, Mathematical Sciences Research Institute, Berkeley, CA

E-mail address: Lomonaco@UMBC.EDU

URL: http://www.csee.umbc.edu/~lomonaco

University of Illinois at Chicago, Chicago, IL 60607-7045

E-mail address: Kauffman@UIC.EDU

URL: http://www.math.uic.edu/~kauffman