QUANTUM CONVOLUTION AND QUANTUM CORRELATION ALGORITHMS ARE PHYSICALLY IMPOSSIBLE

CHRIS LOMONT

Abstract. The key step in classical convolution and correlation algorithms, the componentwise multiplication of vectors after initial Fourier Transforms, is shown to be physically impossible to do on quantum states. Then this is used to show that computing the convolution or correlation of quantum state coefficients violates quantum mechanics, making convolution and correlation of quantum coefficients physically impossible.

1. Introduction

The Fast Fourier Transform (FFT) is arguably the most important algorithm in computer science. Many applications, from image processing, signal processing, pattern matching, polynomial multiplication, number multiplication, and many others are accomplished efficiently by utilizing the FFT to compute a Discrete Fourier Transform (DFT) of some set of data (see [4, Chapter 32] and [7, Chapter 3]). Naively, the DFT of $N = 2^n$ complex values has complexity $O(N^2)$, but the famous paper by Cooley and Tukey [3] introduced the Fast Fourier Transform, reducing the complexity to $\Theta(N \log N) = \Theta(n2^n)$, making Fourier transforms extremely useful in computer algorithms. This efficiency is the basis of fast convolution and correlation algorithms, which do a DFT on each input sequence, then a componentwise multiplication, then an inverse DFT, computing convolution or correlation with complexity $O(N \log N)$.

In the last decade, quantum computing has become well known due to the integer factoring algorithm of Shor [9] and the database search of Grover [8], both of which have complexities much better than their classical counterparts. There are other problems [10] for which quantum computers perform exponentially better than any classical (Turing) computer. A quantum Fourier Transform (QFT) can be done on a quantum state consisting of $N = 2^n$ complex values with complexity $O(\log^2 N) = O(n^2)$ (see for example, [2, Chapter 5]), making it exponentially faster than the classical counterpart, but unfortunately the peculiarities of quantum mechanics disallows using this algorithm as a direct replacement for all FFT algorithms. In fact, after the breakthrough algorithms of Shor and Grover, no algorithms of similar importance have been found, although there has been intense work in this direction.

Since the QFT and inverse QFT are more efficient than their classical counterparts, and the FFT and inverse FFT are the cornerstones for convolution and

Date: Aug 20, 2003.
2000 *Mathematics Subject Classification.* 03D15, 81P10, 81P68, 68W10, 68Q05.
Key words and phrases. algorithms, quantum computers, Fourier transforms, convolution, correlation, information theory.
Research supported by AFRL grant F30602-03-C-0064.

correlation algorithms, it is reasonable to attempt to construct quantum analogues of convolution and correlation algorithms that outperform their classical counterparts. *The key point of this paper is that there is no physically realizable method to compute the normalized convolution or correlation of the coefficients of two quantum states.* Thus replacing classical algorithms that rely on convolution or correlation cannot be done in a simple, direct algorithm replacement manner, but must be approached by more sophisticated techniques, avoiding the method examined in this paper. The precise definitions of quantum convolution and quantum correlation are in section 3, and it is shown in section 4 that they cannot be computed without violating quantum mechanics.

2. Background

Since this paper touches upon several areas, we review some key ideas to make it clearer for readers coming from different backgrounds. In particular, we will recall how convolution and correlation are done classically, followed by a review of rules for quantum computation, sufficiently covered for our needs. Then we will state the convolution and correlation problem for quantum states. Finally, we will prove such an approach is doomed to fail, since it would allow a violation of quantum mechanics.

2.1. Classical convolution and correlation.

Convolution and correlation have many uses in algorithms, which we will not go into here. Since different authors and fields of study use slightly different definitions for the following terms, we define them here, and choose a form amenable to making quantum versions. In particular, different authors use different factors where the $\sqrt{N}$ appears in our definitions, depending on how they will use them. We choose the conventions below to make our definitions mimic the quantum versions in section 2.2.1, where the factors are dictated by unitarity.

Definition 1 (Discrete Fourier Transform). *Given a sequence $\alpha_0, \alpha_1, \ldots, \alpha_{N-1}$ of N complex numbers, the* **Discrete Fourier Transform** *(DFT) of the sequence is defined to be the sequence $a_0, a_1, \ldots, a_{N-1}$ given by*

$$a_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \alpha_k e^{2\pi i jk/N} \quad j = 0, 1, \ldots, N-1$$

Definition 2 (Inverse DFT). *Given a sequence $a_0, a_1, \ldots, a_{N-1}$ of N complex numbers, the* **Inverse Discrete Fourier Transform** *(IDFT) of the sequence is defined to be the sequence $\alpha_0, \alpha_1, \ldots, \alpha_{N-1}$ given by*

$$\alpha_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j e^{-2\pi i jk/N} \quad k = 0, 1, \ldots, N-1$$

The IDFT and DFT are inverses, so are 1-1 on sequences.

Definition 3 (Convolution). *The* **convolution** *of two sequences of N complex numbers $S_1 = (\alpha_0, \alpha_1, \ldots \alpha_{N-1})$ and $S_2 = (\beta_0, \beta_1, \ldots \beta_{N-1})$ is defined to be the sequence $S_3 = (\gamma_0, \gamma_1, \ldots, \gamma_{N-1})$ given by*

$$\gamma_k = \sum_{j=0}^{N-1} \alpha_j \beta_{k-j} \quad \textit{for} \quad k = 0, 1, \ldots N-1$$

where subscripts are taken $\pmod N$*.*

Definition 4 (Correlation)**.** *The* **correlation** *of two sequences of N complex numbers $S_1 = (\alpha_0, \alpha_1, \dots \alpha_{N-1})$ and $S_2 = (\beta_0, \beta_1, \dots \beta_{N-1})$ is defined to be the sequence $S_3 = (\gamma_0, \gamma_1, \dots, \gamma_{N-1})$ given by*

$$\gamma_k = \sum_{j=0}^{N-1} \alpha_j^* \beta_{k+j} \quad \textit{for} \quad k = 0, 1, \dots N-1$$

where α_j^* is the complex conjugate of α_j and subscripts are taken $\pmod N$*.*

2.1.1. *Convolution/correlation algorithm.* It is a simple exercise to check that an algorithm to compute the convolution (or correlation) of two length N sequences in time $O(N \log N)$ is:

(1) FFT - apply the FFT to each sequence in time $O(N \log N)$, giving two sequences of length N.
(2) Multiply - multiply the resulting sequences componentwise in time $O(N)$, assuming each entry can be multiplied in constant time. If doing correlation, conjugate the first FFT sequence in time $O(N)$.
(3) Invert - Apply the inverse FFT to the resulting sequence with time complexity $O(N \log N)$, and multiply each number by $\sqrt{N}$, giving the convolution sequence.

2.2. **The rules of quantum computing.** A quantum system is determined by a quantum state vector, often denoted $|\psi\rangle$. Mathematically, a quantum state on n two-state particles (each called a qubit) is a unit vector in a $N = 2^n$ dimensional complex Hilbert space. For the rest of this paper N will be 2^n for some positive integer n. The Hilbert space is equipped with an orthonormal basis labelled $|i\rangle$, for $i = 0, 1, \dots, N-1$. This state is written as

$$|\psi\rangle = \sum_{i=0}^{N-1} a_i |i\rangle$$

where the a_i are complex numbers, $|i\rangle$ is the i^{th} orthonormal basis element, and the a_i satisfy the *normalization condition* $\sum_i |a_i|^2 = 1$. Quantum mechanics allows two methods to change the state of a system:

(1) **Unitary transformations**. Any state change of an isolated system must be reversible, and must satisfy the normalization condition above, which leads to unitary operations on the state. That is, a state $|\psi\rangle$ can be transformed to the state $U|\psi\rangle$ via the unitary matrix U. Unitary means $U^\dagger U = I = UU^\dagger$ where I is the identity matrix, and $\dagger$ is the conjugate transpose.
(2) **Measurement operators**. Applying a measurement to a quantum state returns an "answer" with a probability related to the magnitude of the coefficients, and places the system into the state whose value was returned from the measurement. Precisely, a quantum measurement consists of a collection $\{M_m\}$ of *measurement operators*, which must satisfy $\sum_m M_m^\dagger M_m = I$ to preserve probability. When applied to a system $|\psi\rangle$, with probability

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

the state becomes the state

$$|\psi\rangle \xrightarrow{M_m} \frac{M_m|\psi\rangle}{\sqrt{p(m)}}$$

and outcome m is observed by the measurement. See [2, Chapter 2] for details and examples.

(3) **Combining states** The concatenation of two quantum systems on n and m qubits with states $|\psi\rangle$ and $|\phi\rangle$ respectively is the tensor product state $|\psi\rangle \otimes |\phi\rangle$ in complex 2^{n+m} dimensional space. Shorthand is

$$\left(\sum_i a_i|i\rangle\right) \otimes \left(\sum_j b_j|j\rangle\right) = \sum_{i,j} a_i b_j |ij\rangle$$

For the purpose of this paper it is necessary to define what we mean by "physically realizable computation". There are many approaches to this question, but for our purposes it is enough to take a very general definition, under which we show convolution and correlation to be impossible, since they remain impossible under more confining and precise definitions. A quantum computation can utilize extra states called "ancillary qubits" as working space, so we allow a finite number of extra qubits to be used internally to the system.

Definition 5 (Physically realizable)**.** *A mapping P of quantum states*

$$|\phi\rangle \quad \xrightarrow{P} \quad |\psi\rangle$$

is called **physically realizable** *if there exists a finite fixed sequence of unitary transformations and measurement operators and a quantum state $|\rho\rangle$ (called the ancillary qubits) performing the mapping. That is, for all $|\phi\rangle$, the fixed sequence S performs the mapping*

$$|\phi\rangle \otimes |\rho\rangle \quad \xrightarrow{S} |\psi\rangle$$

Note in particular, the mapping is a composition of linear operators, so is a linear operator. There are some researchers working on nonlinear quantum mechanics, but there is no experimental evidence to date that supports nonlinearity [6]. One interesting result is that if quantum mechanics is nonlinear, then quantum computers can solve NP-complete and #P problems in polynomial time [1], which some believe is very good evidence that quantum mechanics is strictly linear. For our purposes we use the standard view that quantum mechanics has linear evolution.

2.2.1. *The Quantum Fourier Transform.* Similar to the classical Fourier Transform and inverse defined in section 2.1, we can define quantum analogues, operating on sequences of complex numbers stored as quantum state coefficients.

Definition 6 (Quantum Fourier Transform)**.** *The* **Quantum Fourier Transform** *(QFT) is the unitary map defined on basis states $|j\rangle$ as*

$$|j\rangle \quad \xrightarrow{QFT} \quad \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

and extended by linearity.

Definition 7 (Inverse QFT)**.** *The* **Inverse Quantum Fourier Transform** *(IQFT) is the unitary map defined on basis states $|k\rangle$ as*

$$|k\rangle \quad \xrightarrow{IQFT} \quad \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{-2\pi ijk/N}|j\rangle$$

and extended by linearity.

Note 8. It is easy to check these are inverses on quantum states, and that each transform is unitary.

The quantum state $|\psi\rangle = \sum a_i|i\rangle$ then transforms as

$$\sum_{j=0}^{N-1} a_j|j\rangle \quad \xrightarrow{QFT} \quad \sum_j a_j \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle \tag{1}$$

$$= \quad \sum_k \left(\frac{1}{\sqrt{N}} \sum_j a_j e^{2\pi ijk/N} \right) |k\rangle \tag{2}$$

One reason some quantum algorithms are superior to classical ones is that the QFT has complexity $O(\log^2 N) = O(n^2)$ [2, Chapter 5], *which is exponentially faster than the classical $O(n2^n)$ version!* It is precisely this exponential speedup that allows Shor's integer factoring algorithm to out-perform the best known classical one.

3. Problem Statement

In this section we describe an attempt to construct quantum versions of the convolution and correlation algorithms, based on the classical algorithms 2.1.1. Since the QFT operates on quantum coefficients, we will encode the sequences in a quantum state, with the sequence entries stored in the coefficients. Since a quantum state $\sum_i \alpha_i|i\rangle$ requires $\sum_i |\alpha_i|^2 = 1$, we require each sequence to have at least one nonzero entry, and then we normalize the sequence to have norm 1. We ignore the physical method the quantum state is constructed from the sequence, since the many ways to construct it would lead us. So we have a (hypothetical) method of converting a nonzero sequence of complex numbers into a representative quantum state.

The problems become:

Definition 9 (The Quantum Convolution Problem)**.** *Given quantum states representing the two initial sequences, compute a quantum state representing the convolution sequence. That is, given the two states (for $N = 2^n$)*

$$|\alpha\rangle \quad = \quad \sum_{i=0}^{N-1} \alpha_i|i\rangle \tag{3}$$

$$|\beta\rangle \quad = \quad \sum_{j=0}^{N-1} \beta_j|j\rangle \tag{4}$$

compute a state

$$|\gamma\rangle = \sum_{k=0}^{N-1} \gamma_k|k\rangle \tag{5}$$

where $|\gamma\rangle$ *represents the normalization of the sequence given by*

$$c_k = \sum_{j=0}^{N-1} \alpha_j \beta_{k-j} \quad \textit{for } k = 0, 1, \ldots N-1 \tag{6}$$

and subscripts are taken $\pmod N$.

Definition 10 (The Quantum Correlation Problem)**.** *Given quantum states representing the two initial sequences, compute a quantum state representing the correlation sequence. That is, given the two states (for* $N = 2^n$*)*

$$|\alpha\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle \tag{7}$$

$$|\beta\rangle = \sum_{j=0}^{N-1} \beta_j |j\rangle \tag{8}$$

compute a state

$$|\gamma\rangle = \sum_{k=0}^{N-1} \gamma_k |k\rangle \tag{9}$$

where $|\gamma\rangle$ *represents the normalization of the sequence given by*

$$c_k = \sum_{j=0}^{N-1} \alpha_j^* \beta_{k+j} \quad \textit{for } k = 0, 1, \ldots N-1 \tag{10}$$

and subscripts are taken $\pmod N$.

Note 11. For each definition to make sense, the resulting sequence c_k cannot be all zeros. This can be guaranteed by requiring that the initial sequences are each not all zero, and then padding each initial sequence by appending N zeros. Then, choose i_0 and j_0 each minimal so that $\alpha_{i_0} \neq 0$ and $\beta_{j_0} \neq 0$. Then $c_{i_0+j_0} = \alpha_{i_0}\beta_{j_0} \neq 0$ in the convolution sequence. Pick i_1 maximal so that $\alpha_{i_1} \neq 0$, then $c_{j_0-i_1} = \alpha_{i_1}^*\beta_{j_0} \neq 0$ in the correlation sequence, with subscripts taken $\pmod N$. Padding by N zeros requires adding only one more qubit, so we assume for the rest of this paper that this is the case. Then each problem is well-defined. This changes each problem slightly, but proving impossibility in these slightly amended case suffices to prove impossibility in general.

4. Impossibility proof

This section gives a proof that the problems given in definitions 9 and 10 cannot be computed by any device obeying quantum mechanics. Precisely, we prove in section 4.3:

Theorem 12 (Impossibility of quantum convolution)**.** *There is no physically realizable process P to compute the (normalized) convolution of the coefficients of two quantum states. That is, for arbitrary quantum states* $\sum_i a_i|i\rangle$ *and* $\sum_j b_j|j\rangle$*, there is no physically realizable process P to compute the state*

$$\sum_{i,j=0}^{N-1} a_i b_j |ij\rangle \xrightarrow{P} \lambda \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} a_j b_{k-j} |k\rangle \tag{11}$$

where $\lambda = 1/\sqrt{\sum |a_i b_j|^2}$ *is the normalization factor, subscripts are taken* $\pmod N$, *and* $N = 2^n$ *for some integer* $n > 0$.

and

Theorem 13 (Impossibility of quantum correlation)**.** *There is no physically realizable process* P *to compute the (normalized) correlation of the coefficients of two quantum states. That is, for arbitrary quantum states* $\sum_i a_i|i\rangle$ *and* $\sum_j b_j|j\rangle$, *there is no physically realizable process* P *to compute the state*

$$\sum_{i,j=0}^{N-1} a_i b_j |ij\rangle \xrightarrow{P} \lambda \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} a_j^* b_{k+j} |k\rangle \tag{12}$$

where $\lambda = 1/\sqrt{\sum |a_i b_j|^2}$ *is the normalization factor, subscripts are taken* $\pmod N$, *and* $N = 2^n$ *for some integer* $n > 0$.

This is done in several parts. First, we show that step 2 in algorithm 2.1.1 has no quantum analogue by studying requirements on a linear transformation that attempts step 2. Then we show no physical process consisting of arbitrary sequences of unitary operations and measurements can perform step 2. This proves that step 2 is impossible to compute on quantum states. Finally, we show that any physical process able to compute quantum convolution or correlation as in definitions 9 and 10 would be able to compute the impossible step 2, a contradiction. Thus there can be no quantum convolution or correlation done on quantum states.

4.1. **Linearity considerations.** Suppose we try to obtain the componentwise product of two states, using some linear operator on the initial state. Heuristically, this should fail, since all components in the outcome may be zero. Even if we remove this case (which is reasonable, see note 11), we show such an operation is still not possible. Since linear operators encompass both unitary operations and measurement systems, we analyze the linear operator case first. As in definition 5, we allow the algorithm to use arbitrary finite "workspace" in the form of a third quantum state $\sum_k c_k|k\rangle$ on m qubits in order to show the problem cannot even be computed with extra working space.

Lemma 14. *There is no linear operator* L *and a quantum state* $\sum c_k|k\rangle$ *such that for arbitrary quantum states* $\sum a_i|i\rangle$ *and* $\sum b_j|j\rangle$ *with* $\sum |a_i b_i| \neq 0$, *the following operation is performed on quantum states:*

$$\sum_{i,j,k} a_i b_j c_k |ijk\rangle \xrightarrow{L} \left(\lambda \sum_i a_i b_i |i\rangle\right) \otimes \left(\sum_{j,k} d_{jk} |jk\rangle\right) \tag{13}$$

where the d_{jk} *are functions of the* a_i, b_j, *and* c_k, *with* $\sum |d_{jk}|^2 = 1$, *and* $\lambda = 1/\sqrt{\sum_i |a_i b_i|^2}$ *is a normalization factor.*

Proof. Assume there is a linear operator L and initial state $\sum_k c_k|k\rangle$ satisfying 13. Write L as

$$L = \sum_{\substack{a,b,c\\r,s,t}} e_{rstabc} |rst\rangle\langle abc|$$

and apply it to the initial state to get

$$\left(\sum_{\substack{a,b,c\\r,s,t}} e_{rstabc}|rst\rangle\langle abc|\right)\left(\sum_{i,j,k} a_i b_j c_k |ijk\rangle\right) = \sum_{\substack{r,s,t\\i,j,k}} a_i b_j c_k e_{rstijk}|rst\rangle \tag{14}$$

We want this state to equal the desired outcome, giving

$$\sum_{\substack{r,s,t\\i,j,k}} a_i b_j c_k e_{rstijk}|rst\rangle = \lambda \sum_{r,s,t} a_r b_r d_{st}|rst\rangle \tag{15}$$

Looking at the $|0st\rangle$ component, we require for a fixed s,t that

$$\lambda a_0 b_0 d_{st} = \sum_{i,j,k} a_i b_j c_k e_{0stijk} \tag{16}$$

Equation 16 must hold for any a_i and b_j coefficients giving a quantum state. Fix $\epsilon \in (0,1)$, and pick sequences of coefficients as

$$\{a_i\} = \{\epsilon, \sqrt{1-\epsilon^2}, 0, 0, 0 \ldots, 0\} \tag{17}$$

$$\{b_j\} = \{1, 0, 0, \ldots, 0\} \tag{18}$$

Then $\lambda = 1/\epsilon$, $a_0 b_0 = \epsilon$, $a_1 b_0 = \sqrt{1-\epsilon^2}$, and $a_i b_j = 0$ for all other i, j combinations. Equation 16 becomes

$$d_{st} = \epsilon \sum_k c_k e_{0st00k} + \sqrt{1-\epsilon^2} \sum_k c_k e_{0st01k} \tag{19}$$

$$= \epsilon C_1 + \sqrt{1-\epsilon^2} C_2 \tag{20}$$

where C_1 and C_2 are constants depending on the initial choices for L and c_k. Normalization requires

$$1 = \sum_{s,t} |d_{s,t}|^2 \tag{21}$$

$$= \sum_{s,t} |\epsilon C_1 + \sqrt{1-\epsilon^2} C_2|^2 \tag{22}$$

$$= MN\left(\epsilon^2 C_1^2 + 2\epsilon\sqrt{1-\epsilon^2} C_1 C_2 + (1-\epsilon^2) C_2^2\right) \tag{23}$$

$$= MNC_2^2 + \epsilon^2 MN(C_1^2 - C_2^2) + 2\epsilon\sqrt{1-\epsilon^2} MNC_1 C_2 \tag{24}$$

Equation 24 must hold true for all $\epsilon \in [0,1]$. When $\epsilon = 0$, the last two terms are zero, forcing $C_2 = 1/\sqrt{MN} \neq 0$. When $\epsilon = 1$, the last term is zero, and the middle term must be zero, forcing $C_2^2 = C_1^2 \neq 0$. Now the middle term is zero for all ϵ. However, when $\epsilon = 1/2$, equation 24 is a contradiction, so there can be no linear operator L and initial state $\sum c_k|k\rangle$ satisfying 13 for arbitrary input states.

$\square$

Note lemma 14 is a purely mathematical statement, driven by physical requirements, and cast in quantum mechanics language. The following variation is used later to prove the impossibility of quantum correlation.

Corollary 15. *There is no linear operator L and a quantum state $\sum c_k|k\rangle$ such that for arbitrary quantum states $\sum a_i|i\rangle$ and $\sum b_j|j\rangle$ with $\sum |a_ib_i| \neq 0$, the following operation is performed on quantum states:*

$$\sum_{i,j,k} a_ib_jc_k|ijk\rangle \xrightarrow{L} \left(\lambda \sum_i a_i^* b_i|i\rangle\right) \otimes \left(\sum_{j,k} d_{jk}|jk\rangle\right) \tag{25}$$

with $\sum |d_{jk}|^2 = 1$, and $\lambda = 1/\sqrt{\sum_i |a_ib_i|^2}$ is a normalization factor.

Proof. The proof is the same as lemma 14, since the sequences needed in the proof were real numbers. □

4.2. **Unitary transforms and measurements fail.**

Theorem 16. *There is no physical process P capable of either of the transformations*

$$\sum_{i,j} a_ib_j|ij\rangle \xrightarrow{P} \lambda \sum_i a_ib_i|i\rangle \tag{26}$$

$$\sum_{i,j} a_ib_j|ij\rangle \xrightarrow{P} \lambda \sum_i a_i^* b_i|i\rangle \tag{27}$$

on arbitrary quantum states with $\sum |a_ib_i| \neq 0$, where λ is a normalization factor.

Proof. Since unitary transforms are linear operators, both lemma 14 and corollary 15 remain true when the phrase "linear operator L" is replaced with "unitary transform L". So no single unitary operation L can perform either transformation. Similarly, a measurement operator $\{M_m\}$ is a collection of linear transforms on a quantum state, so no single measurement operator can perform either transformation. Finally, given any (finite) sequence of unitary operations and measurement operations, we can always apply all the unitary operations first, and then apply the measurements, by the "Principle of Deferred Measurement" [2, Chapter 4]. Then the unitary operations compose to a single unitary operation, and the measurements combine to form a single measurement operation [2, Exercise 2.57]. A unitary operation U followed by a measurement operator $\{M_m\}$ is the measurement operator $\{UM_m\}$, which also cannot perform either transformation. So there is no physical process P to perform either transform. □

4.3. **Quantum convolution and correlation are impossible.** Finally, we can prove the main theorems 12 and 13:

Proof of theorem 12. Suppose such a process P existed. Then the composition $(IQFT \otimes IQFT) \circ P \circ QFT$ is physically realizable, which performs transformation 26 in theorem 16, a contradiction.

Thus there can be no physically realizable quantum convolution process. □

Note: this proof could use the fact that P would be linear, as would the composition, which would contradict lemma 14.

Proof of theorem 13. The proof is the same as the proof of theorem 12 with minor changes. Thus there can be no physically realizable quantum correlation process. □

5. Conclusion and open problems

We have shown there is no physical way to compute the convolution or correlation on quantum states. This is unfortunate for many applications, yet there may remain ways to attack specific sequences which yield efficient quantum algorithms. For example, it is possible to use a measurement to compute the transform $\sum a_i b_j |ij\rangle \to \lambda \sum a_i b_i |ii\rangle$, but the probability of obtaining this state tends to 0 as $N \to \infty$, likely rendering it useless in algorithms.

A final interesting point is that given a sequence of numbers on a classical computer, we could compute a convolution, and prepare the quantum states in lemma 14, which seems to violate theorem 16. The point is that once the input sequences are in the quantum states, without knowing the classical information so we can make copies, there is no way to get the output state. Quantum states cannot be copied by the No Cloning Theorem [5, 11], otherwise the transform of theorem 16 could be computed by sampling enough copies of the input to determine the classical sequences, classically computing the convolution, then constructing the output state. This approach is prevented by the No Cloning Theorem. The key point is that storing a classical information theory sequence of numbers into the quantum state coefficients is not a reversible process, since there is no way to read all the coefficients back out of the state.

A final note: this result was inspired by a comment made by David Meyer, who obtained similar results independently.

References

1. Daniel S. Abrams and Seth Lloyd, *Nonlinear quantum mechanics implies polynomial-time solution for NP-complete and #P problems*, Phys.Rev.Lett. **81** (1998), 3992–3995.
2. I. L. Chuang and M. A. Nielsen, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.
3. James W. Cooley and John W. Tukey, *An algorithm for the machine calculation of complex fourier series*, Math. Comput. **19**, 297–301,.
4. Thomas Cormen, Charles Leiserson, Ronald Rivest, and Clifford Stein, *Introduction to Algorithms, Second Edition*, MIT Press, 2001, ISBN: 0262032937.
5. D. Dieks, *Communication by EPR devices*, Phys. Lett. A **92** (1982), no. 6, 271–272.
6. P. K. Majumder et. al., Phys.Rev.Lett. **65** (1990), 2931.
7. Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, Addison-Wesley, 1992, ISBN: 0201508036.
8. L. K. Grover, *A fast quantum mechanical algorithm for database search*, Proc. 28th Ann. ACM Symp. on Theory of Comput., 1996, pp. 212–219.
9. P. W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings, 35th Annual Symposium on Fundamentals of Comp. Science (FOCS), 1994, pp. 124–134.
10. David R. Simon, *On the power of quantum computation*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Los Alamitos, CA), Institute of Electrical and Electronic Engineers Computer Society Press, 1994, pp. 116–123.
11. W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802–803.

E-mail address: `clomont@cybernet.com, clomont@math.purdue.edu`

URL: `www.math.purdue.edu/~clomont`

Current address: Cybernet Systems Corporation, 727 Airport Blvd., Ann Arbor, MI, 48108-1639 USA.