# Extension of quantum factoring applying white noise analysis

R. ASGHARI*
*Faculties of Information, Communication and Technology, Malek -Ashtar University of Technology, Tehran, Iran.*

In the present paper Shor's factoring algorithm is studied with white noise analysis. Generalized functionals are developed in order to express registers and Fourier transform is developed for generalized functions. Using white noise analysis Shor's factoring algorithm is extended to more than two entangled registers in Hilbert spaces. Based on the presented generalization, Generalized Shor's factoring algorithm with two and more registers are presented.

(Received July 11, 2017; accepted April 5, 2018)

*Keywords*: White noise analysis, Quantum mechanics, Quantum fourier transform, Factoring algorithm

## 1. Introduction

Over the recent years by the advent of huge size computational problems, quantum computing has become a very popular field among scientists with different disciplines, such as physicists, engineers, and mathematicians [1] . Quantum computation owes most of the attraction to the famous Shor's period-finding algorithm, which leads to an efficient algorithm for factoring integers in polynomial time.

It is well known that the security of the most widely used public-key cryptosystems such as RSA [1, 2] is based on number-theoretic problems so called the integer factorization. There are other number theoretic cryptosystems e.g. [2, 3] recently developed and none of them can be solved applying polynomial-time algorithms, which makes the cryptosystems based on them secure. There are, however, quantum algorithms, due to Shor [4,5], which can solve the NP hard factoring problems in polynomial time [6]. Shor's Factoring algorithm is developed in quantum mechanics and is simulated in quantum computers in recent decays for very small numbers [7,8,9].

It seems that the development of quantum computers is serious as time going by the dream goes to be true, which can be addressed by recent directed researches in laser and other related parts of the physics [10,11,12]. By the advent of quantum computers, the definition of security will changed. Alongside quantum computers that Factoring in polynomial times, Quantum Key Distribution protocols will also developed, using the quantum nature [13].

Based on the factoring algorithm and a few new concepts in quantum mechanics, many new quantum algorithms have been developed in recent decades. The quantum algorithms have been designed to run on two registers created by a finite dimensional state space. In the case of Shor's factoring algorithm, which is basis for many quantum algorithms and is the main inspiration for designing quantum computers, recently researchers have been directed their attention toward developing the Algorithm on more registers [14] that operates on state spaces of infinite dimension [15,16].

The main objective of developing the continuous version of the Shor's factoring or other quantum algorithms are to make them more mathematically transparent, by extending the inner workings of his original quantum factoring algorithm [17]. continuous variable analogue of other quantum algorithms are also developed; teleportation [18], secrecy sharing [19], entanglement [20], error correction [21].

Continuous version of other famous quantum algorithm such as Grover's algorithm [22] and Deutsch-Jozsa algorithm was recently created [23] was also developed.

The continuous version of the Shor's Factoring algorithm is began by the work of [17] which applied the methods found in [15] to create a continuous variable analogue of Shor's quantum factoring algorithm. They developed quantum hidden subgroup algorithm that finds the period of a function $\Phi : R \to R$ where $\Phi$ is generalized function called admissible function.

Recently Becnel [16] developed a framework based on white noise analysis and extended Shor's factoring algorithm in hidden subspace for infinite dimensions. His framework in quiet interesting from mathematical point of view and inspired us in the present paper. The present paper is based on the works of Becnel [16,24] and intending to apply the concepts of white noise analysis to develop a Shor's algorithm in infinite dimensional Hilbert spaces. Based on [24] we applied weak topology on countable tensor product of Hilbert spaces to define generalized functions for constructing generalized registers and applied generalized version of Fourier transform applied in Shor' factoring algorithm. From this point of view and as one of the goals of the paper, the continuous version of the algorithm for more than two registers is also developed. One can see that this extension to more registers is straight forward in this continuous framework.

The paper is organized as follows; in section 2 the original Shor's factoring algorithm is presented for the case of three and more registers, in section 3 white noise analysis is presented for developing generalized functions, in section 4 generalized Fourier transform is presented, in section 5 generalized Shor's factoring algorithm is presented for the case of two and more registers and finally in section 6 convolution is drawn.

## 2. Algorithm with more Registers

In this section we review the discrete case of the Shor's factoring algorithm with more registers which is discussed in [14]. We consider Quantum order finding (the Quantum part of the Shor's algorithm) for $a$ with respect to $N$;

Given an integer $n = 2m+1+[\log(2+\frac{1}{2\epsilon})]$, setting $n$ qubits initialized to 0, $m$ qubits initialized to the state $|1\rangle$. The goal is to find the least integer $p$ such that $a^p \equiv 1(\mathrm{mod}N)$ [17]:

1. Put register-1 in the following uniform superposition state by applying $H^{\otimes n} \otimes I \otimes I$ :

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle |1,1\rangle,$$

2. Perform Fourier transform $\mathcal{F} \otimes I \otimes I$ to the superposition:

$$\frac{1}{\sqrt{q2^n}} \sum_{s=0}^{p-1} \sum_{k=0}^{2^n-1} \exp(2\pi iks/p) |k\rangle |x^s \ (\mathrm{mod}\, N), x^s (\mathrm{mod} N)\rangle$$

3. Apply inverse Fourier transform $\mathcal{F}^{-1} \otimes I \otimes I$ on register-1. The state becomes

$$\sum_{s=0}^{p-1} (\frac{s}{p}) |x^s \ (\mathrm{mod}\, N), x^s (\mathrm{mod}\, N)\rangle,$$

4. Observe register-1, with respect to basis $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ : $\frac{s}{p}$ the same interpretation is presented for the case of $l$ dimensional entangled registers. In this case the inputs are same as 3 register case, we summarize two main steps of the Quantum order finding algorithm in the following :

1. Put register-1 in the following uniform superposition state

$$\frac{1}{\sqrt{q}} \sum_{k=0}^{2^n-1} |k\rangle |\underbrace{1,1,\ldots,1}_{l}\rangle,$$

2. Perform Fourier transform $\mathcal{F} \otimes I \otimes \ldots \otimes I$ to the superposition:

$$\frac{1}{\sqrt{q2^n}} \sum_{s=0}^{p-1} \sum_{k=0}^{2^n-1} \exp(2\pi iks/p) \times |k\rangle |\underbrace{x^s \ (\mathrm{mod}\, N), x^s (\mathrm{mod}\, N), \ldots, x^s (\mathrm{mod}\, N)}_{l}\rangle,$$

3. Apply inverse Fourier transform $\mathcal{F}^{-1} \otimes \underbrace{I \otimes \ldots \otimes I}_{l}$ on register-1. The state becomes

$$\sum_{s=0}^{p-1} (\frac{s}{p}) |\underbrace{x^s \ (\mathrm{mod}\, N), \ldots, x^s (\mathrm{mod}\, N)}_{l}\rangle,$$

4. Observe register-1,

At the rest of the paper we are going to state a framework to generalize the algorithm applying white noise analysis.

## 3. The White Noise Analysis

In order Let $H$ be a Hilbert space equipped with the norm $\|.\|_H$ , and consider an operator $\mathcal{A}$ on $H$ . Get the orthonormal basis $\{e_n\}_{n=1}^{\infty}$ on $H$ with the following properties:

$$\mathcal{A}e_n = \lambda_n e_n \quad (1)$$

$$1 \le \lambda_1 \le \lambda_1 \le \ldots \le \lambda_n \le \ldots \quad (2)$$

$$\sum_{n=1}^{\infty} \lambda_n^{-2} < \infty a1 \le \lambda_1 \le \lambda_1 \le \ldots \le \lambda_n \le \ldots \quad (3)$$

Noting that by conditions (1) and (2) $\mathcal{A}^{-1} a_1 \le \lambda_1 \le \lambda_1 \le \ldots \le \lambda_n \le \ldots$ is a bounded operator on $H$ and by (3) $\mathcal{A}^{-1}$ is Hilbert-Schmidt on $H$ [24]. We define the Hilbert space $E_j = \mathcal{A}^{-j}(H)$ which has the form:

$$E_j = \{x \in H : \sum_{n \ge 0} \lambda_n^{2j} |\langle x, e_n \rangle|^2\}$$

with natural inner product $\langle f, g \rangle_j = \langle \mathcal{A}^j f, \mathcal{A}^j g \rangle$ generalized from the space $H$ [28, 29]. Now the following chain can be constructed

$$E = \bigcap_{j \in N_0} E_j \subset \ldots \subset E_2 \subset E_1 \subset H, \quad (4)$$

where $N_0$ is set of natural numbers containing $0$. Now one can see that the inclusion $E_{j+1} \subseteq E_j$ is Hilbert-Schmidt. Let us equip the space $E$ with the topology generated by the norms induced by the inner products $\{\langle .,. \rangle_j\}_{j=0}^{\infty}$. Since $E$ is nuclear space (the vectors $e$ all lie in $H$ and the set of all rational linear combinations of these vectors produces a countable dense subspace of $E$), then the topological dual $E'$ is the union of all duals $E'_j$.

$$E' = \bigcup_{j \in N_0} E'_j \supset \ldots \supset E_2 \supset E_1 \supset H' \equiv H, \quad (5)$$

with the inner product $\langle f, g \rangle_{-j} = \langle \mathcal{A}^{-j} f, \mathcal{A}^{-j} g \rangle$ again is generalized from $H$ [30]. Now by (4) and (5) we can state the Gel'fand triple $E \subseteq H \subseteq E'$.

One can construct a probability measure $\mu_\sigma$ on the Borel $\sigma$-algebra of subsets of the dual $E'$, generated by the map $H \to L^2(E', \mu) : \xi \to \hat{\xi}$ with the following property:

$$\int_{E'} e^{is\hat{\xi}(x)} d\mu_\sigma = e^{-s^2\sigma^2 \| \xi \|_H^2 / 2}$$

for every $s$ and $\xi$ in $H$. This is a Gaussian measure and is applied in the following inner products.

Applying multiple Wiener-Ito integral $I_j = H^{\otimes j} \to L^2(E', \mu)$, where $H^{\otimes j}$ is a Hilbert space spanned by $h_1 \otimes h_2 \otimes \ldots \otimes h_j$ in which $h_n$ for $n = 1, 2, \ldots j$ belongs to $H$. Noting that the tensor product can be constructed in the way that we obtain symmetric tensor products [16,24,30]. Now by Wiener-Ito theorem each $\hat{f} \in L^2(E', \mu)$ can be uniquely expressed as $\hat{f} = \sum_{j=0}^{\infty} I_j(f_j)$, for $f_j \in H^{\otimes j}$. We also denote the space of all $(f_j)_{j=1}^{\infty}$ where $\sum_{j=1}^{\infty} j! \| f_j \|_H^2 < \infty$. By $Y(H)$ which equipped with inner product $\langle f, g \rangle_Y = \sum_{i=1}^{\infty} i! \langle f, g \rangle_H$.

The operator $\mathcal{B}$ on $L^2(E', \mu)$ can be defined applying the operator $\mathcal{A}$, but first we need to define an orthonormal basis on $L^2(E', \mu)$. The basis can be defined by

$$\tilde{e}_{j_1, j_2, \ldots} \equiv \frac{1}{\sqrt{j_1! j_2! \ldots}} I_n(e_1^{\otimes j_1} \otimes e_2^{\otimes j_2} \otimes \ldots) \quad (6)$$
$$j_1 + j_2 + \ldots = j$$

where $e_n^{\otimes j_n}$ is orthonormal basis for $H^{\otimes j_n}$ and

$$I_j(e_1^{\otimes j_1} \otimes e_2^{\otimes j_2} \otimes \ldots) = \mathcal{H}_{j_1}(\langle ., e_1 \rangle) \mathcal{H}_{j_2}(\langle ., e_2 \rangle) \ldots,$$

with Hermit polynomials of degree $n$:

$$\mathcal{H}_n = (-1) e^{\frac{x^2}{2}} \frac{d^n}{dx^n} e^{\frac{-x^2}{2}}.$$

Now getting the operator $\mathcal{B}$ and orthonormal basis $\{\tilde{e}_{j_1, j_2, \ldots}; j_1 + j_2 + \ldots = j, j = 0, 1, 2, \ldots\}$ for $L^2(E', \mu)$ we have

$$\mathcal{B}\tilde{e}_{j_1, j_2, \ldots} = (\lambda_1^{j_1} \lambda_2^{j_2} \ldots) \tilde{e}_{j_1, j_2, \ldots}.$$

It is possible to verify that $\mathcal{B}$ satisfies condition (2) and (3) analogous to $\mathcal{A}$ and therefore is Hilbert-Scmidt operator. As a result one can be able to construct the sequence of spaces $\mathcal{E}_j = \{ f \in L^2(E', \mu); \| f \|_j < \infty \}$, where $\| . \|_j$ is norm on $\mathcal{E}_j$ induced by the inner product $\langle\langle f, g \rangle\rangle_j = \langle \mathcal{B}^j f, \mathcal{B}^j g \rangle_Y$.

Then the space $\mathcal{E} = \bigcap_{j \in N_0} \mathcal{E}_j$ can be achieved in analogous way. With the topology induced by norms $\{\| . \|_j\}_{j=0}^{\infty}$, the dual $\mathcal{E}'$ of $\mathcal{E}$ is obtained equal to $\bigcup_{j \in N_0} \mathcal{E}'_j$ which leads to the following Gel'fand triple $\mathcal{E} \subseteq L^2(E', \mu) \subseteq \mathcal{E}'$ in an analogous way [25, 26]. Therefore, everything is ready to construct generalized functions on $\mathcal{E}'$ with natural dual pairing $\langle\langle ., . \rangle\rangle$ between $\mathcal{E}$ and $\mathcal{E}'$.

Defining Hermit polynomials of degree $n$ with parameter $\sigma$ by

$$\mathcal{H}_\sigma^n(x) = (-\sigma^2)^n e^{\frac{x^2}{2\sigma^2}} \frac{d^n}{dx^n} e^{\frac{-x^2}{2\sigma^2}}$$

One can construct $\mathcal{H}_\sigma^{\otimes j}$ on tensor product spaces, then for $x \in \mathcal{E}'$ and $y \in \mathcal{E}$ one can check that [16]:

$$\langle \mathcal{H}_\sigma^{\otimes j}(x), y^{\otimes j} \rangle = \sum_{n=0}^{j/2} \binom{j}{2k} (2k-1)!! (- \| y \|_H^2) \langle x, y \rangle.$$

For $f_j \in H^{\otimes j}$, with Wiener-Ito integral we have:

$$I_n(f)(x) = \langle \mathcal{H}_\sigma^{\otimes j}(x), f \rangle, \qquad \forall x \in \mathcal{E}' \qquad (7)$$

then by (7), $\varphi \in L^2(\mathcal{E}', \mu)$ can be represented as:

$$\hat{f}(x) = \sum_{j=0}^{\infty} \langle \mathcal{H}_\sigma^{\otimes j}(x), f_j \rangle, \quad \forall x \in \mathcal{E}'$$

where $f_j \in H^{\otimes j}$ and $\sum_{j=0}^{\infty} \langle \mathcal{H}_\sigma^{\otimes j}(x), f_j \rangle \in \mathcal{E}^{\otimes j}$ which implies $\hat{f} \in \mathcal{E}_j$. These relations lets us to create a proper correspondence between the spaces $H^{\otimes j}$ and $\mathcal{E}_i^{\otimes j}$, which is crucial for defining generalized function in $\mathcal{E}'$. To this end we get the following orthonormal basis for $L^2(E', \mu)$ from (1.3);

$$\tilde{e}_{j_1, j_2, \ldots}(x) = \frac{1}{\sqrt{j_1! j_2! \ldots}} \langle \mathcal{H}_\sigma^{\otimes j}(x), e_1^{\otimes j_1} \otimes e_2^{\otimes j_2} \otimes \ldots \rangle, \qquad j_1 + j_2 + \ldots = j,$$

then we are going to construct the eigen equation

$$\mathcal{B}\tilde{e}_{j_1, j_2, \ldots}(x) = \frac{1}{\sqrt{j_1! j_2! \ldots}} \langle \mathcal{H}_\sigma^{\otimes j}(x), \mathcal{A}^{\otimes n}(e_1^{\otimes j_1} \otimes e_2^{\otimes j_2} \otimes \ldots) \rangle, \qquad j_1 + j_2 + \ldots = j$$

Likewise we define the space of all functions $\varphi = (\mathbf{f}_j)_{j=0}^{\infty}$ with $\sum_{j=0}^{\infty} j! \| \mathbf{f}_j \|_{-j} < \infty$ by $\mathbf{Y}(E')$ Now for $f_j \in E^{\otimes j}$ we construct the test functions $\phi(x) = \sum_{j=1}^{\infty} \langle \mathcal{H}_\sigma^{\otimes j}(x), f_j \rangle$ which belongs to $\mathcal{E}_i$ .

We define the generalized function $\Psi$ that for all $\phi \in \mathcal{E}$ as a weak solution of the following equation;

$$\langle\langle \Psi(x), \phi \rangle\rangle = \sum_{j=1}^{\infty} e^{-\frac{\| x \|_H}{2}} j! \langle \mathbf{f}_j, f_j \rangle.$$

Then the generalized function $\Psi \in \mathcal{E}'$ can be constructed as

$$\Psi(x) = \sum_{j=0}^{\infty} e^{-\frac{\| x \|_H}{2}} \langle \mathcal{H}_\sigma^{\otimes j}(x), \mathbf{f}_j \rangle$$

which has meaning only in weak sense and is called Wiener-Ito expression of generalized function. with this construction of the generalized function, we are ready to express the quantum Fourier transform and delta function required in the computations.

## 4. Generalized Fourier transform and delta function

We aim to define Fourier transform of generalized function $\Psi$ in the space $\mathcal{E}'$. The Fourier transform of a function $f$ is defined as:

$$\mathcal{F}(f)(y) = (2\pi)^{-n/2} \int_{\mathbb{R}^n} e^{-i\langle x, y \rangle + |x|^2/2} f(x) e^{-|x|^2/2} dx.$$

In order to define Fourier transform of a generalized function by Wiener-Ito representation, get $y \in E'$ then in $\mathcal{E}'$ we have generalized function $\sum_{i=0}^{\infty} \frac{1}{n!} \langle \mathcal{H}_\sigma^{\otimes n}(x), y^{\otimes n} \rangle$ which let us to define Fourier transform of a generalized function $\Psi \in \mathcal{E}'$ analogous to ordinary version: $\mathcal{F}\Psi(y) = \int_{E'} \sum_{j=0}^{\infty} e^{-\frac{\| x \|_H}{2}} \frac{1}{j!} \langle \mathcal{H}_\sigma^{\otimes j}(x), y^{\otimes j} \rangle \Psi(x) d\mu(x)$ but this is a symbolic formulation. The Fourier transform of generalized function can be computed in week sense as follows:

$$\langle\langle \Psi, e^{-i\langle x, \xi \rangle} \rangle\rangle = \sum_{j=0}^{\infty} e^{-\frac{\| \xi \|_H}{2}} i^j \langle \mathbf{f}_j, \xi^{\otimes j} \rangle, \qquad \forall \xi \in E$$

where $e^{-i\langle x, \xi \rangle}$ is applied as test function.

For delta function likewise we are going to represent Wiener-Ito expression. For every test function $\phi \in \mathcal{E}$ we have the following Wiener-Ito expression: $\sum_{j=0}^{\infty} \langle \mathcal{H}_\sigma^{\otimes j}(x), f_j \rangle$ .

Then applying Kubo-Yokoi delta function gives

$$\langle\langle \delta_x, \phi \rangle\rangle = \phi(x) = \sum_{j=0}^{\infty} \langle \mathcal{H}_\sigma^{\otimes j}(x), f_j \rangle.$$

Another interesting result is applying test function

$\phi' = \sum_{j=0}^{\infty} \frac{1}{j!} \langle \mathcal{H}_\sigma^{\otimes j}(x), y^{\otimes j} \rangle$ with $y \in E'$ gives

$$\langle\langle \delta_x, \phi' \rangle\rangle = \phi'(x) = \sum_{j=0}^{\infty} \frac{1}{j!} \langle \mathcal{H}_\sigma^{\otimes j}(x), y^{\otimes j} \rangle.$$

## 5. Generalized Shor's factoring algorithm

Based on the concepts presented in this paper, generalized Shor's factoring algorithm is developed in this sections. The concept of rigged Hilbert space is applied in the following is denoted by $H_{R^n}$ which is space of functions $f$ on $R^n$ that is $f \neq 0$ on only countable number of points and $\sum_{x \in R^n} |f(x)| < \infty$. Natural inner product

$$\langle f, g \rangle = \sum_{x \in R^n} f(x) g(x)$$

is stated on the space. $H_{R^n}$ is non-separable Hilbert space and $|x\rangle = 1_x$ with $\langle x \mid y \rangle = \delta_{xy}$ is an orthonormal basis on it. In order to prepare initial superposition of states it is needed to define an unitary operator

$$U : L^2(E', \mu) \otimes H_{R^n} \to L^2(E', \mu) \otimes H_{R^n}$$

with the following property:

$$U(\Psi \otimes |x\rangle) = \Psi \mid x + \phi(f_1)\rangle.$$

where $\phi : H \to R^n$ is a functional and $f_1$ comes from unique Wiener-Ito representation

$$\Psi(x) = \sum_{j=0}^{\infty} e^{-\frac{\|x\|_H}{2}} \langle \mathcal{H}_\sigma^{\otimes j}(x), f_j \rangle$$

where $f_j \in H^{\otimes j}$. The algorithm with two registers is outlined in Algorithm 1.

**Algorithm 1**

Generalized Shor's factoring algorithm with two registers

Step 1: Get the unite vector (Generalized function) $\Psi$ in $L^2(E', \mu)$ and set the initial state to

$S_0 = \Psi \mid 0\rangle$

noting that $S_0 \in L^2(E', \mu) \otimes Y(H)$

Step 2: In this step the unitary operator $U$ is applied for creating superposition of states:

$$S_1 = U(S_0) = \Psi \mid \phi(f_1)\rangle$$

where $f_1 \in E$ comes from Wiener-Ito representation.

Step 3: Generalized Fourier transform is applied on the generalized function $\Psi$. That is we apply the operator $\mathcal{F} \otimes I$ on $S_1$:

$S_2 = (\mathcal{F} \otimes I)(S_1) = (\mathcal{F} \otimes I)\Psi \mid \phi(f_1)\rangle = \mathcal{F}\Psi \mid \phi(f_1)\rangle$

Step 4: Applying inverse Fourier transform by operator $\mathcal{F}^{-1} \otimes I$ to get

$S_3 = (\mathcal{F}^{-1} \otimes I)(S_2)$

$= (\mathcal{F}^{-1} \otimes I)\mathcal{F}\Psi \mid \phi(f_1)\rangle$

$= \Psi \mid \phi(f_1)\rangle$

### 5.1. Extending Generalized Shor's algorithm for more registers

By the formulation the stated in the paper we can directly extend the generalized version of the Shor's factoring to more registers. Assuming that $2 < l \in N$ registers are considered, the we need unitary operator

$$\tilde{U} : L^2(E', \mu) \otimes H_{R^n}^{\otimes l} \to L^2(E', \mu) \otimes H_{R^n}^{\otimes l}$$

in the way that

$$\tilde{U}(\Psi \otimes |\underbrace{x \mid x \mid \ldots \mid x}_{l}\rangle)$$

$$= \Psi \mid \underbrace{x + \phi(f_1) \mid x + \phi(f_1) \mid \ldots \mid x + \phi(f_1)}_{l}\rangle.$$

The algorithm with $l$ registers is outlined in Algorithm 2.

**Algorithm 2**

Generalized Shor's factoring algorithm with registers

Step 1: Get the unite vector (Generalized function) $\Psi$ in $L^2(E', \mu)$ and set the initial state to

$$S_0 = \Psi \mid \underbrace{0 \mid 0 \mid \ldots \mid 0}_{l}\rangle$$

noting that $S_0 \in L^2(E', \mu) \otimes Y^{\otimes l}(H)$.

Step 2: Unitary operator $\tilde{U}$ is applied to get:

$$S_1 = \tilde{U}(S_0) = \Psi \mid \underbrace{\phi(f_1) \mid \phi(f_1) \mid \ldots \mid \phi(f_1)}_{l}\rangle$$

where $f_1 \in E$ comes from Wiener-Ito representation.

Step 3: Generalized Fourier transform is applied on the generalized function $\Psi$ That is we apply the operator $\mathcal{F} \otimes I^{\otimes l}$ on $S_1$:

$$S_2 = (\mathcal{F} \otimes I^{\otimes l})(S_1)$$
$$= (\mathcal{F} \otimes I^{\otimes l})\Psi \,|\, \underbrace{\phi(f_1)\,|\,\phi(f_1)\,|\ldots|\,\phi(f_1)}_{l}\rangle$$
$$= \mathcal{F}\Psi \,|\, \underbrace{\phi(f_1)\,|\,\phi(f_1)\,|\ldots|\,\phi(f_1)}_{l}\rangle$$

Step 4: Applying inverse Fourier transform by operator $\mathcal{F}^{-1} \otimes I^{\otimes l}$ to get

$$S_3 = (\mathcal{F}^{-1} \otimes I^{\otimes l})(S_2)$$
$$= (\mathcal{F}^{-1} \otimes I^{\otimes l})\mathcal{F}\Psi \,|\, \phi(f_1)\rangle$$
$$= \Psi \,|\, \underbrace{\phi(f_1)\,|\,\phi(f_1)\,|\ldots|\,\phi(f_1)}_{l}\rangle$$

## 6. Measurements

In quantum version of the Shor's factoring algorithm measurements is done by collapsing the state In order to do measurement we take a random non-zero vector $\xi \in H$ and let $\Psi$.

We need to define a specific space to project the measuring state in order to keep required properties. The desired space is with $\overline{\mathcal{M}}$ where

$$\mathcal{M} = \text{span}\{\langle \mathcal{H}_\sigma^{\otimes j}, f_j \rangle; f_j \in H^{\otimes j}, j = 1,2,\ldots\}$$

then the orthogonal projection $P_{\mathcal{M}}^j$ for $j = 1,2,\ldots$ with $P_{\mathcal{M}}^j P_{\mathcal{M}}^k = \delta_{jk} P_{\mathcal{M}}^k$ is the required measurement is performed with respect to $\{P_{\mathcal{M}}^j\}_{j=0}^{\infty}$ by

$$P_{\mathcal{M}}^j(\Psi) = e^{-\frac{\|\xi\|_H}{2}} \frac{1}{j!} \langle \mathcal{H}_\sigma^{\otimes j}, \xi^{\otimes j} \rangle$$

by this measurement we can extract $\xi \in E$ .

$$\Psi = \sum_{j=0}^{\infty} e^{-\frac{\|\xi\|_H}{2}} \frac{1}{j!} \langle \mathcal{H}_\sigma^{\otimes j}(x), \xi^{\otimes j} \rangle$$

## 7. Conclusion

The paper considers the Shor's factoring algorithm on infinite dimensional Hilbert spaces and for two and more registers. The generalization is done based on white noise analysis which is developed recently to define generalized function for constructing registers in continuous case and developed Fourier transform as well as delta function in weak sense. The framework is simply developed the case of more than two registers for Shor's Factoring algorithm. This framework can be applied for other quantum algorithms such as Deutsch-Jozsa or error correction algorithms.

## References


[1] R. L. Rivest, A. Shamir, L. Adleman, Communications of the ACM **21**(2), 120 (1978).

[2] B. F. Vajargah, R Asghari, International Journal of Mechatronics, Electrical and Computer Technology (IJMEC) **5**(15), 2026 (2015).

[3] B. F. Vajargah, R Asghari, Indian Journal of Science and Technology **9**(6), (2016).

[4] P. Shor, SIAM J. Comput. **26**(5), 1484 (1997).

[5] P. Shor, Introduction to quantum algorithms, AMS PSAPM **58**, 143 (2002).

[6] S. Y. Yan, Quantum attacks on public-key cryptosystems, Springer, 2013.

[7] L. M. K. Vandersypen, M. Steffen , G. Breyta, C. S. Yannoni, M. H. Sherwood, I. L. Chuang, Nature **414**, 883 (2001).

[8] C. Y. Lu, D. E. Browne, T. P. Yang, W. Jian, Physical Review Letters **99**(25), 250 (2007).

[9] S. S. Li, G. L. Long, F. S. Bai, S. L. Feng, H. Z. Zheng, Proceedings of the National Academy of Sciences **98**(21), 11847 (2001).

[10] A. Armaselu, Optoelectron. Adv. Mat. **9**(3-4), 531 (2015).

[11] B. F. Vajargah, R Asghari, J. Optoelectron. Adv. M. **19**(1-2) , 109 (2017) .

[12] N. Celebi, Optoelectron. Adv. Mat. **7**(3-4), 188 (2013).

[13] M. Dima, M. Dulea, D. O. Aranghel, P. Sterian, Optoelectron. Adv. Mat. **4**(11), 1840 (2010).

[14] Z. Cao, C. Zhenfu, "On Shor's Factoring Algorithm with More Registers and the Problem to Certify Quantum Computers," arXiv preprint arXiv:1409.7352 (2014).

[15] J. Samuel Lomonaco Jr , L. H. Kauffman, Quantum hidden subgroup problems: A mathematical perspective, AMS CONM, 305, 2002.

[16] J. J. Becnel, Extension of Shor's period-finding algorithm to infinite dimensional Hilbert spaces, Ph.D. Dissertation, Louisiana State University, 2006.

[17] J. Samuel Lomonaco Jr., L. H. Kauffman, A continuous variable Shor algorithm, arXiv preprint quant-ph/0210141, 2002.

[18] S. L. Braunstein, H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).

[19] O. Pfister, F. Sheng, G. Jennings, R. Pooser, D. Xie, Physical Review A **70**(2), 020302(R) (2004).

[20] T. Tomas, B. C. Sanders, Phys. Rev. A **65**, 042310 (2002).

[21] D. Gottesman, A. Kitaev, J. Preskill, Physical Review A **64**(1), 012310 (2001).

[22] A. K. Pati, S. L. Braunstein, S. Lloyd, Quantum searching with continuous variables, arXiv preprint quant-ph/0002082, 2000.

[23] A. K. Pati, S.L. Braunstein, Quantum Information with Continuous Variables, Springer Netherlands, 31-36, 2003.

[24] J. J. Becnel, Transactions of the American Mathematical Society **364**(10), 5035 (2012).
[25] J. J. Becnel, Proceedings of the American Mathematical Society **134**(2), 581 (2006).
[26] J. J. Becnel, A. Sengupta, Proceedings of the American Mathematical Society **135**(9), 2995 (2007).
[27] M. Eslami, F. S Khodadad, F. Nazari, H Rezazadeh, Optical and Quantum Electronics **49**(12), 391 (2017).
[28] M. Eslami, H. Rezazadeh, M. Rezazadeh, S. S Mosavi, Optical and Quantum Electronics **49**(8), 279 (2017).
[29] A. Neirameh, M. Eslami, Scientia Iranica **24**(2), 715 (2017).
[30] M. Eslami, Applied Mathematics and Computation **285**, 141 (2016).

*Corresponding author: meisam.mathhome@gmail.com