# Transformadas Quânticas de Fourier e de Hartley

Bernardo Lula Jr., Bruno B. Albert e Francisco M. de Assis

***Resumo*— Uma descoberta notável ocorrida na área da teoria da informação e computação quântica foi a prova de existência de um algoritmo quântico para fatoração de inteiros de $n-$ bits com complexidade $\mathcal{O}(n^2 \log n \log\log n)$ operações. Este algoritmo é exponencialmente mais eficiente que o melhor algoritmo clássico correspondente que exige $\mathcal{O}(\exp(n^{1/3}\log^{2/3}))$ operações. A razão para a eficiência do algoritmo quântico mencionado é a existência de um algoritmo para o cálculo da transformada de Fourier quântica (QFT) de complexidade $\mathcal{O}((\log N)^2)$ enquanto o melhor algoritmo clássico (FFT) tem complexidade $\mathcal{O}(N \log N)$ para uma instância de tamanho $N$ (em geral $N = 2^n$). Este artigo focaliza de modo tutorial a QFT e introduz as transformadas de Hartley quânticas definindo-as e verificando algumas de suas propriedades mais importantes.**

***Palavras-Chave*— Tranformada discreta de Fourier quântica, transformada discreta de Hartley quântica.**

***Abstract*— A remarkable discovery inside quantum information and quantum computation areas was the proof of existence of an effective quantum algorithm to find prime factorization of $n-$ bit integers with complexity $\mathcal{O}(n^2 \log n \log\log n)$ operations. Such that algorithm is exponentially more efficient that the best corresponding classical algorithm that requires $\mathcal{O}(\exp(n^{1/3}\log^{2/3}))$ operations. The reason for such quantum algorithm impressive efficacy is the existence of an algorithm to calculate the quantum Fourier transform (QFT) with complexity $\mathcal{O}((\log N)^2)$, while the best classical (FFT) corresponding algorithm has complexity $\mathcal{O}(N \log N)$ for instances of size $N$(in general $N = 2^n$). This article focus like a tutorial on QFTs and focus on quantum Hartley transforms introducing them and verifying some of their more important properties.**

***Keywords*— Quantum Fourier transform, Quantum Hartley transform**

## I. Introdução

No computador, tal como conhecido hoje, a informação é representada por grandezas que obedecem as leis da física clássica tais como níveis de tensão e ciruitos lógicos. Paul Benioff, no início da decada de 80, e mais tarde Richard Feynman vislumbraram a possibilidade de usar grandezas representadas pela mecânica quântica para o desenvolvimento de algoritmos computacionais. O estado quântico representando um bit de informação é chamado de bit quântico ou simplesmente *qubit*. Duas polarizações distintas de um fóton pode ser um exemplo de um qubit no estado 0 ou no estado 1.

Como em circuitos lógicos tem-se as portas lógicas, no lado quântico tem-se as portas lógicas quânticas que realizam operações sobre o estado de um ou mais qubits. Estas operações são a base para a construção de um computador quântico. No entanto, devido ao princípio da superposição na mecânica quântica, os qubits podem assumir outros estados diferentes dos estados clássicos 0 e 1. Com isso o computador quântico pode realizar operações de modo mais eficiente que o computador clássico que utilize operações booleanas convencionais.

Peter Shor mostrou, em 1994 [1], que um computador quântico pode encontrar os fatores primos de um número composto de modo mais eficiente do que um computador convencional. Como a fatoração de inteiros está na base dos sistemas criptográficos de chave pública modernos, o resultado de Shor torna esses sistemas obsoletos uma vez que o computador quântico seja uma realidade. Dessa forma pesquisadores têm investido um esforço considerável na determinação da classe de problemas que são passíveis de um aumento na velocidade quando são colocados sob o ponto de vista quântico.

Como elemento básico do algoritmo de Shor, e de vários outros algoritmos quânticos interessantes, está a transformada de Fourier discreta quântica (QFT), definida de maneira similar a transformada de Fourier discreta clássica (DFT). A QFT é introduzida de modo tutorial na Seção III. A principal contribuição deste artigo é a verificação de algumas propriedades da transformada discreta de Hartley quântica (QHT), cuja correspondente clássica apresenta propriedades interessantes para certas aplicações. Até onde vai o conhecimento dos autores, a QHT ainda não está sendo explorada nos algoritmos quânticos.

O artigo está organizado da seguinte forma: na Seção II apresenta-se de maneira suscinta os fundamentos da mecânica quântica, a notação utilizada e uma descrição das portas quânticas; na Seção III são mostradas as transformadas quânticas discreta de Fourier e de Hartley provando algumas de suas propriedades. Finalmente na Seção IV apresenta-se uma conclusão do trabalho.

## II. Notação e Fundamentos

Grande parte da teoria da mecânica quântica está baseada na álgebra linear e equações diferenciais. Entretanto, sob o ponto de vista da teoria da informação e computação quânticas, essa teoria pode ser encarada como um conjunto de postulados sobre espaços vetoriais de Hilbert [2]. Na mecânica quântica utiliza-se freqüentemente a notação de Dirac, bastante eficiente na descrição dos sistemas quânticos.

Matematicamente, um estado quântico em um espaço complexo de Hilbert de dimensão $N = 2^n$ é representado por um vetor de dimensão $N$ designado por $|\psi\rangle$. Nesta notação o elemento $|.\rangle$ é chamado de *ket*. Se o vetor $|j\rangle$, para $j = 0, 1, \ldots, N-1$, representar um elemento da base ortonormal de um espaço de Hilbert, então pode-se escrever

$$|\psi\rangle = \sum_{j=0}^{N-1} a_j |j\rangle \tag{1}$$

Bernardo Lula Jr., Departamento de Sistemas e Computação. Bruno B. Albert e Francisco M. de Assis. Departamento de Engenharia Elétrica, Universidade Federal de Campina Grande, Campina Grande, Brasil, E-mails: lula@dsc.ufcg.edu.br, albert@dee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br.

em que $a_j$ são números complexos e devem satisfazer a condição de normalização $\sum_j |a_j|^2 = 1$. Na notação padrão da mecânica quântica, o produto interno entre dois vetores $|v\rangle$ e $|w\rangle$, pertencentes a um espaço vetorial, é representado por $\langle v|w\rangle$, em que $\langle v|$ é a notação usada para o vetor dual do vetor $|v\rangle$. Também define-se um produto externo, que é útil na representação de operadores lineares. Seja $|v\rangle$ e $|u\rangle$ vetores do espaço de Hilbert $V$ e $|w\rangle$ um vetor do espaço de Hilbert $W$, então o produto externo $|w\rangle\langle v|$ é um operador linear de $V$ em $W$ definido por

$$(|w\rangle\langle v|)|u\rangle \triangleq |w\rangle\langle v|u\rangle = \langle v|u\rangle|w\rangle. \tag{2}$$

A evolução de um sistema quântico isolado se dá por meio de tranformações unitárias que devem ser reversíveis. Assim, dado um estado $|\psi\rangle$, ele pode evoluir para o estado $U|\psi\rangle$ por meio do operador (matriz) unitário $U$. O operador ser unitário significa que $UU^\dagger = U^\dagger U = I$, em que $I$ representa o operador identidade e $\dagger$ é o conjugado transposto. O operador $U^\dagger$ é chamado de adjunto ou conjugado hermitiano do operador $U$.

Finalmente, a concatenação de dois estados quânticos de dimensões $N = 2^n$ e $M = 2^m$ representados por $|\psi\rangle$ e $|\varphi\rangle$ respectivamente é o produto tensorial entre esses dois estados definido por

$$\begin{aligned} |\psi\rangle \otimes |\varphi\rangle &= \left(\sum_i a_i|i\rangle\right) \otimes \left(\sum_j b_j|j\rangle\right) \\ &= \sum_{i,j} a_i b_j |i\rangle|j\rangle \\ &= \sum_{i,j} a_i b_j |ij\rangle \end{aligned} \tag{3}$$

em que $|ij\rangle$ é um vetor no espaço de dimensão $2^{n+m}$.

### A. Portas Quânticas

Tal como os computadores clássicos são constituídos por portas lógicas, também os computadores quânticos podem ser representados por portas quânticas que podem ser conectadas para realizar um determinado algoritmo. Uma maneira conveniente de se representar uma porta quântica é na forma matricial. A seguir são apresentadas algumas dessas portas quânticas.

As portas que atuam sobre um único qubit podem ser repesentadas por matrizes $2\times2$. As três portas definidas abaixo estão entre as mais importantes e são chamadas de matrizes de Pauli.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4}$$

Estas portas transformam o estado $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, nos estados

$$\begin{aligned} X|\psi\rangle &= a_0|1\rangle + a_1|0\rangle \\ Y|\psi\rangle &= i(a_0|1\rangle - a_1|0\rangle) \\ Z|\psi\rangle &= a_0|0\rangle - a_1|1\rangle \end{aligned} \tag{5}$$

A porta X é a chamada de porta **NOT** pela sua equivalência com a porta **NOT** clássica. Três outras portas quânticas também são importantes, e são mostradas a seguir

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}. \tag{6}$$

Estas portas transformam o estado $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, nos estados

$$\begin{aligned} H|\psi\rangle &= a_0\frac{|0\rangle + |1\rangle}{\sqrt{2}} + a_1\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ S|\psi\rangle &= (a_0|0\rangle + ia_1|1\rangle) \\ T|\psi\rangle &= a_0|0\rangle + e^{i\pi/4}a_1|1\rangle \end{aligned} \tag{7}$$

A porta H é chamada de porta de Hadamard, a porta S de porta de fase e a porta T de porta $\pi/8$. É bom lembrar que todas essas matrizes são unitárias, ou seja, preservam a norma do qubit.A Figura II-A mostra a representação de uma porta de um único qubit, em que o U representa uma das portas (X, Y, Z, H, S ou T).

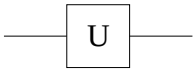


Fig. 1. Representação de uma porta quântica para um único qubit

Das portas quânticas que atuam em dois (ou mais) qubits, a mais conhecida é a porta **NOT** -controlada ou **CNOT** . Nesta porta, mostrada na Figura II-A, a linha de cima representa o qubit de controle e a outra linha representa o qubit alvo. A

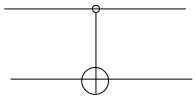

Fig. 2. Representação da porta **NOT** -controlada

ação da porta pode ser descrita da seguinte forma, se o qubit de controle for 0, então o qubit alvo não é alterado, agora se o qubit de controle for 1 o qubit alvo é negado, (equivalente a passar por uma porta **NOT** ). Esta porta pode servista como uma generalização da porta clássica **XOR** , assim uma outara maneira de se descrever a porta **CNOT** é através da expressão

$$|i, j\rangle \longrightarrow |i, i \oplus j\rangle, \tag{8}$$

em que $\oplus$ significa adição módulo-2.

## III. Transformadas Quânticas

A técnica das transformadas é amplamente conhecida com inúmeras aplicações. Como será visto a seguir algumas transformadas clássicas têm uma versão quântica e um dos pontos que chamam a atenção é que elas podem ser calculadas mais rapidamente em um computador quântico que suas versões clássicas em um computador convencional. Nesta seção são apresentadas duas dessas transformadas, a transformada discreta de Fourier quântica e a transformada discreta de Hartley quântica fazendo um paralelo com suas versões clássicas.

### A. Transformada Discreta de Fourier Quântica

Dado um vetor $\mathbf{x} = (x_0, x_1, \ldots, x_{N-1})$ de dimensão $N$, em que $x_i \in \mathcal{C}$ o conjunto dos complexos, a transformada discreta de Fourier de $\mathbf{x}$ é um vetor com componentes complexas $\mathbf{y} = (y_0, y_1, \ldots, y_{N-1})$ também de dimensão $N$, em que cada componente $y_k$ é calculada da seguinte forma

$$y_k \triangleq \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \tag{9}$$

e sua inversa

$$x_j \triangleq \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k e^{-2\pi ijk/N}. \tag{10}$$

De forma similar define-se o par de transformadas discretas de Fourier quânticas sobre uma base ortonormal $|j\rangle$ como um operador linear $\mathcal{F}$, usando a notação quântica

$$\mathcal{F}|j\rangle \triangleq \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \tag{11}$$

e sua inversa

$$\mathcal{F}^{-1}|k\rangle \triangleq \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi ijk/N} |j\rangle. \tag{12}$$

Para provar que a equação (12) é realmente a QFT inversa deve-se mostrar que $\mathcal{F}^{-1}\mathcal{F}|j\rangle = |j\rangle$, mas antes necessita-se de um resultado preliminar, apresentado a seguir.

*Lema 1:* Sejam $j, k, L \in \mathbf{Z}$, em que $\mathbf{Z}$ representa o conjunto dos inteiros, então

$$\sum_{j=0}^{L-1} e^{2\pi ijk/L} = \begin{cases} L & \text{se } L|k, \\ 0 & \text{caso contrário,} \end{cases} \tag{13}$$

em que $L|k$ significa que $L$ divide $k$.

*Demonstração:* Se $L|k$ então $k/L = n$ com $n \in \mathbf{Z}$, assim

$$\begin{aligned} \sum_{j=0}^{L-1} e^{2\pi ijk/L} &= \sum_{j=0}^{L-1} \left(e^{2\pi ik/L}\right)^j \\ &= \sum_{j=0}^{L-1} \left(e^{2\pi in}\right)^j \\ &= \sum_{j=0}^{L-1} 1 = L. \end{aligned} \tag{14}$$

Se $L$ não divide $k$, então

$$\begin{aligned} \sum_{j=0}^{L-1} e^{2\pi ijk/L} &= \sum_{j=0}^{L-1} \left(e^{2\pi ik/L}\right)^j \\ &= \frac{\left(e^{2\pi ik/L}\right)^L - 1}{e^{2\pi ik/L} - 1} \\ &= 0, \end{aligned} \tag{15}$$

nesta última passagem utilizou-se a seguinte igualdade $\sum_{j=0}^{N-1} x^j = (x^N - 1)/(x - 1)$. ■

Continuando, então,

$$\begin{aligned} \mathcal{F}^{-1}\mathcal{F}|j\rangle &= \mathcal{F}^{-1}\left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle\right) \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} \mathcal{F}^{-1}|k\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} e^{-2\pi ikm/N}|m\rangle \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \sum_{m=0}^{N-1} e^{2\pi i(j-m)k/N}|m\rangle \\ &= \frac{1}{N} \sum_{k=0}^{N-1} |j\rangle + \frac{1}{N} \sum_{\substack{m=0 \\ m\neq j}}^{N-1} \sum_{k=0}^{N-1} e^{2\pi i(j-m)k/N}|m\rangle \\ &= |j\rangle. \end{aligned} \tag{16}$$

Observe que o somatório interno do somatório duplo, na útima passagem, é zero pelo Lema 1 pois $N$ não divide $k$.

Para um estado arbitrário $|\psi\rangle = \sum_{j=0}^{N-1} x_j|j\rangle$ qualquer, tem-se

$$\begin{aligned} \mathcal{F}|\psi\rangle &= \mathcal{F}[\sum_{j=0}^{N-1} x_j|j\rangle] \\ &= \sum_{j=0}^{N-1} x_j \mathcal{F}|j\rangle \\ &= \sum_{j=0}^{N-1} x_j \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle \\ &= \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}\right)|k\rangle \\ &= \sum_{k=0}^{N-1} y_k|k\rangle, \end{aligned} \tag{17}$$

em que os valores $y_k$ representam a transformada discreta de Fourier dos valores $x_j$.

O operador transformada discreta de Fourier quântica é um operador unitário. Este fato pode ser provado por duas maneiras, uma prova direta ou através de um circuito quântico unitário que realize a transformada. A prova direta é apresentada a seguir. O primeiro passo é escrever o operador $\mathcal{F}$ na forma matricial, lembrando que o operador identidade $I$ tem a seguinte forma matricial $I = \sum_{j=0}^{N-1} |j\rangle\langle j|$ em que $|j\rangle$ é um vetor da base ortonormal do espaço vetorial de dimensão $N$,

$$\begin{aligned} \mathcal{F} &= I\mathcal{F}I \\ &= \sum_s |s\rangle\langle s|\mathcal{F}\sum_t |t\rangle\langle t| \\ &= \sum_{s,t} |s\rangle\langle s|\mathcal{F}|t\rangle\langle t| \\ &= \sum_{s,t} \langle s|\mathcal{F}|t\rangle |s\rangle\langle t|. \end{aligned} \tag{18}$$

Nesta última passagem utilizou-se o fato de $\langle s|\mathcal{F}|t\rangle$ representar um produto interno. Substituindo o valor de $\mathcal{F}|t\rangle$ obtém-se

$$\begin{aligned}\mathcal{F} &= \sum_{s,t}\langle s|\frac{1}{\sqrt{N}}\sum_{k} e^{2\pi itk/N}|k\rangle|s\rangle\langle t| \\ &= \frac{1}{\sqrt{N}}\sum_{s,t,k} e^{2\pi itk/N}\langle s|k\rangle|s\rangle\langle t| \\ &= \frac{1}{\sqrt{N}}\sum_{s,t} e^{2\pi its/N}\langle s|s\rangle|s\rangle\langle t| \\ &= \frac{1}{\sqrt{N}}\sum_{s,t} e^{2\pi its/N}|s\rangle\langle t|.\end{aligned} \tag{19}$$

O segundo passo é achar o conjugado hermitiano de $\mathcal{F}$. Observando o resultado anterior (eq. (19)), obtém-se

$$\mathcal{F}^{\dagger} = \frac{1}{\sqrt{N}}\sum_{s,t} e^{-2\pi its/N}|t\rangle\langle s|. \tag{20}$$

Finalmente, deve-se mostrar que $\mathcal{F}\mathcal{F}^{\dagger} = I$. Assim,

$$\begin{aligned}\mathcal{F}\mathcal{F}^{\dagger} &= \frac{1}{\sqrt{N}}\sum_{s,t} e^{2\pi its/N}|s\rangle\langle t|\frac{1}{\sqrt{N}}\sum_{s,t} e^{-2\pi its/N}|t\rangle\langle s| \\ &= \frac{1}{N}\sum_{s,t}|s\rangle\langle t|t\rangle\langle s| \\ &= \frac{1}{N}\sum_{s,t}|s\rangle\langle s| \\ &= \sum_{s}|s\rangle\langle s| = I.\end{aligned} \tag{21}$$

Uma das características marcantes da QFT em relação a DFT é que a primeira é exponencialmente mais rápida que a segunda. Enquanto que a transformada rápida de Fourier (FFT) tem uma complexidade de $\mathcal{O}(n2^n)$, para $N = 2^n$ valores complexos, a complexidade da QFT é de $\mathcal{O}(n^2)$ [2]. E é precisamente este fato que permite que o algoritmo de fatoração de inteiros de Shor suplante o melhor algoritmo de fatoração clássico conhecido.

Embora a QFT seja mais eficiente que a DFT, duas propriedades importantes na transformada clássica não podem ser realizadas fisicamente no lado quântico: são as operações de convolução e de correlação dos coeficientes de dois estados quânticos [3]. Trabalhos futuros devem contemplar essas limitações da transformadas quânticas apontando alternativas, caso existam.

### *B. Tranformada Discreta de Hartley Quântica*

A transformada discreta de Hartley clássica (DHT) é uma transformada espectral que está estreitamente relacionada com a DFT. A DHT, no entanto, oferece uma série de vantagens em relação a esta última [4], como (i) é uma transformada com valores no conjunto dos reais, (ii) possui a mesma fórmula para a transformada direta e para transformada inversa, (iii) é computacionalmente equivalente a DFT, (iv) exibe uma alta simetria, que é desejável do ponto de vista de implementação e (v) é matematicamente elegante. Isto tem levado a uma série de pesquisas em processamento de sinais no sentido de se usar a DHT em vez da DFT.

Dado um vetor $\mathbf{x}$ de dimensão N com componentes reais, a DHT é definida como um vetor $\mathbf{y}$ de dimensão N cujas componentes são da seguinte forma,

$$y_k \triangleq \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j \operatorname{cas}\left(\frac{2\pi jk}{N}\right), \tag{22}$$

em que $\operatorname{cas}(x) \triangleq \cos(x) + \operatorname{sen}(x)$. Como já foi dito, a sua inversa tem o mesmo formato.

A transformada discreta de Hartley quântica (QHT) é definida de modo similar. Dado um vetor $|j\rangle$, tem-se que

$$\mathcal{H}|j\rangle \triangleq \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \operatorname{cas}\left(\frac{2\pi jk}{N}\right)|k\rangle, \tag{23}$$

com sua inversa definida da mesma forma, como mostrado a seguir. Antes de demonstrar este fato, necessita-se de um resultado que é uma conseqüência direta do Lema 1.

*Corolário 2:* Sejam $j, k, L \in \mathbf{Z}$, então

$$\sum_{j=0}^{L-1}\cos\left(2\pi j\frac{k}{L}\right) = \begin{cases} L & \text{se } L|k, \\ 0 & \text{caso contrário,}\end{cases} \tag{24}$$

e

$$\sum_{j=0}^{L-1}\operatorname{sen}\left(2\pi j\frac{k}{L}\right) = 0. \tag{25}$$

*Demonstração:* Do Lema 1

$$\sum_{j=0}^{L-1}\left[\cos\left(2\pi j\frac{k}{L}\right) + i\operatorname{sen}\left(2\pi j\frac{k}{L}\right)\right] = \begin{cases} L & \text{se } L|k, \\ 0 & \text{caso contrário.}\end{cases} \tag{26}$$

■

Para completar a verificação, é necessária ainda a seguinte

propriedade, $\cas x \cas y = \cos(x-y) + \text{sen}(x+y)$. Assim,

$$\begin{aligned}
\mathcal{H}^{-1}\mathcal{H}|j\rangle &= \mathcal{H}^{-1}\left[\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\cas\left(2\pi j\frac{k}{N}\right)|k\rangle\right] \\
&= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\cas\left(2\pi j\frac{k}{N}\right)\mathcal{H}^{-1}|k\rangle \\
&= \frac{1}{N}\sum_{k=0}^{N-1}\cas\left(2\pi j\frac{k}{N}\right)\sum_{m=0}^{N-1}\cas\left(2\pi m\frac{k}{N}\right)|m\rangle \\
&= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{m=0}^{N-1}\cas\left(2\pi j\frac{k}{N}\right)\cas\left(2\pi m\frac{k}{N}\right)|m\rangle \\
&= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{m=0}^{N-1}\Bigg[\cos\left(2\pi(m-j)\frac{k}{N}\right) \\
&\qquad + \text{sen}\left(2\pi(m+j)\frac{k}{N}\right)\Bigg]|m\rangle \\
&= \frac{1}{N}\sum_{k=0}^{N-1}|j\rangle \\
&\quad + \sum_{\substack{m=0\\m\neq j}}^{N-1}\sum_{k=0}^{N-1}\cos\left(2\pi(m-j)\frac{k}{N}\right)|m\rangle \\
&\quad + \sum_{m=0}^{N-1}\sum_{k=0}^{N-1}\text{sen}\left(2\pi(m+j)\frac{k}{N}\right)|m\rangle \\
&= |j\rangle.
\end{aligned} \tag{27}$$

A última passagem é justificada pelo Colorário 2. A prova de que a QHT assim definida é unitária segue passos semelhantes a prova da QFT (eqs. (18), (19), (20) e (21)). A seguir, são apresentados os passos mais importantes. O operador QHT $\mathcal{H}$ na forma matricial é dado por

$$\begin{aligned}
\mathcal{H} &= I\mathcal{H}I \\
&= \frac{1}{\sqrt{N}}\sum_{s,t}\cas\left(\frac{2\pi st}{N}\right)|s\rangle\langle t|.
\end{aligned} \tag{28}$$

O seu conjugado hermitiano é dado por

$$\mathcal{H}^\dagger = \frac{1}{\sqrt{N}}\sum_{s,t}\cas\left(\frac{2\pi st}{N}\right)|t\rangle\langle s|. \tag{29}$$

Note que, como a QHT é real, $\mathcal{H}^\dagger = \mathcal{H}^T$. Com esses resultados junto com o Corolário 2 obtém-se

$$\begin{aligned}
\mathcal{H}\mathcal{H}^\dagger &= \frac{1}{N}\sum_{s,t}\cas\left(\frac{2\pi st}{N}\right)|s\rangle\langle t|\sum_{s,t}\cas\left(\frac{2\pi st}{N}\right)|t\rangle\langle s| \\
&= \frac{1}{N}\sum_{s,t}\cas^2\left(\frac{2\pi st}{N}\right)|s\rangle\langle t|t\rangle\langle s| \\
&= \frac{1}{N}\sum_{s}|s\rangle\langle s|\sum_{t}\cas^2\left(\frac{2\pi st}{N}\right) \\
&= \frac{1}{N}\sum_{s}|s\rangle\langle s|\sum_{t}\left[1+\text{sen}\left(4\pi s\frac{t}{N}\right)\right] \\
&= \sum_{s}|s\rangle\langle s| = I.
\end{aligned} \tag{30}$$

Um outro resultado interessante da parte clássica que se verifica no lado quântico é que a QHT pode ser escrita em função da QFT, como mostrado a seguir. O núcleo da QHT pode ser escrito como:

$$\begin{aligned}
\cas(x) &= \cos(x) + \text{sen}(x) \\
&= \frac{1-i}{2}e^{ix} + \frac{1+i}{2}e^{-ix}.
\end{aligned} \tag{31}$$

Com esse resultado pode-se reescrever a equação (23) como segue:

$$\begin{aligned}
\mathcal{H}|j\rangle &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\left(\frac{1-i}{2}e^{\frac{2\pi ijk}{N}} + \frac{1+i}{2}e^{\frac{-2\pi ijk}{N}}\right)|k\rangle \\
&= \frac{1-i}{2}\frac{1}{\sqrt{N}}\sum_{k}e^{\frac{2\pi ijk}{N}}|k\rangle + \frac{1+i}{2}\frac{1}{\sqrt{N}}\sum_{k}e^{\frac{-2\pi ijk}{N}}|k\rangle \\
&= \frac{1-i}{2}\mathcal{F}|j\rangle + \frac{1+i}{2}\mathcal{F}^{-1}|j\rangle \\
&= \frac{1-i}{2}\mathcal{F}|j\rangle + \frac{1+i}{2}\mathcal{F}^{3}|j\rangle.
\end{aligned} \tag{32}$$

Observe que foi empregada a propriedade de que a QFT tem ordem quatro, ou seja, $\mathcal{F}^4 = I$. A partir desta definição pode-se observar que a complexidade da QHT é a mesma da QFT, ou seja $\mathcal{O}(n^2)$ [5]. Embora no lado clássico a DHT tenha aplicações em processamento de sinais e de imagem, tais como filtragem e interpolação[6], no lado quântico, apesar de estar formalmente definida, até onde vai o conhecimento dos autores, nenhuma aplicação fez uso da QHT.

## IV. Conclusão

Neste artigo apresentou-se uma introdução às transformadas quânticas definindo formalmente a transformada discreta de Fourier quântica (QFT) e a transformada discreta de Hartley quântica (QHT), demonstrando sua principais propriedades. Enquanto a primeira tem um papel fundamental em vários algoritmos quânticos, como o algoritmo de fatoração de Shor [1], o problema do logaritmo discreto, o problema do subgrupo escondido [8], etc, a segunda, até onde vai o conhecimento dos autores, ainda não tem aplicações definidas na computação quântica.

Embora se tenha discutido apenas essas duas transformadas quânticas, outras já encontram-se definidas na literatura, entre elas as transformadas discretas do seno e do coseno

quânticas [5], as transformadas wavelets quântica [9] e a transformada discreta de Fourier quântica aproximada [10].

## REFERÊNCIAS


[1] Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *35th Annual Symposium on Foundations of Computer Science*, November 1994, Santa Fe, NM.

[2] Michael A. Nielsen and Isac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[3] Chris Lomont, "Quantum convolution and qauntum correlation algorithms are physically impossible," *quant-ph/0309070, submited*, 2003.

[4] R. J. de Sobral Cintra, H. M. de Oliveira, and C. o. Cintra, "The rounded Hartley transform," *International Telecommunications Symposium - ITS2002*, 2002.

[5] Andreas Klappenecker and Martin Rötteler, "On the irresistible efficiency of signal processing methods in quantum computing," *LANL preprint quant-ph/0111039v1*, 2001.

[6] R. P. Millane, "Analitic properties of the hartley transform and their implications," *Proceedings of the IEEE*, vol. 82, no. 3, March 1994.

[7] Richard Jozsa, "Quantum factoring, discrete logarithms, and the hidden subgroup problem," *Computing in Science & Engineering*, 2001.

[8] Peter Hoyer, "Efficient quantum transforms," *LANL preprint quant-ph/9702028*, 1997.

[9] Adriano Barenko, Artur Ekert, and Paivi Toima Kalle-Antti Suominen, "Approximate qauntum fourier transform and decoherence," *Physical Review A, Submitted*, 1996.