Simulação da Transformada Quântica de Fourier

Francisco R. F. Pereira, Elloá B. Guedes, e Francisco M. de Assis

***Abstract*— The quantum Fourier Transform is an important algorithm in Quantum Information Theory due to its capabilities to solve some Quantum Computation and Communication problems. However, so far, no practical quantum computer has been build neither its simulation is efficient on classical computers. Given these difficulties, this paper presents a software able to simulate the quantum Fourier transform – called *FTSimulator* – and also an analysis of its time performance.**

***Keywords*— Quantum Fourier Transform; Simulation; Quantum Algorithms.**

I. Introdução

A *Teoria da Informação Quântica* é um novo paradigma para o processamento e transmissão da informação por considerar as Leis da Física Quântica. Em conseqüência, a informação não encontra-se representada apenas sob a forma de bits, mas também de *qubits* (abreviação de *quantum bits*). Algumas características como *superposição*, *emaranhamento*, *não-clonagem* de estados arbitrários, dentre outras, são próprias deste paradigma e auxiliam na construção de algoritmos para resolução de determinados problemas [1].

Um dos algoritmos de maior destaque nesta área é o *algoritmo quântico de fatoração*, elaborado por Shor [2]. Este algoritmo fatora números de n bits em tempo $O(log^3 n)$, ao passo que nenhuma solução algorítmica conhecida para computadores clássicos (amplamente utilizados nos dias atuais) é capaz de resolver este mesmo problema em tempo menor que exponencial [3]. A proposição deste algoritmo teve um considerável impacto por viabilizar a quebra dos sistemas de segurança baseados em criptografia RSA e também por representar um ganho superpolinomial em relação às suas contrapartidas clássicas [4].

Um dos componentes do algoritmo quântico de fatoração é a *transformada quântica de Fourier* (QFT – *Quantum Fourier Transform*), um algoritmo quântico inspirado na transformada de Fourier, amplamente conhecida e utilizada em diversas áreas da Engenharia. A versão quântica da transformada de Fourier toma como entrada um estado quântico e produz uma superposição de estados quânticos, como formalizado na Definição 1.

Definição 1 (**Transformada Quântica de Fourier**). *Seja $|j\rangle$ um vetor ortonormal em um espaço de Hilbert $\mathcal{H}$ de dimensão 2^m, ou seja, pertencente à base $\{|0\rangle, |1\rangle, \ldots, |2^m - 1\rangle\}$. A transformada quântica de Fourier de $|j\rangle$ é dada por*

$$\mathrm{QFT}\,|j\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} e^{\frac{2\cdot\pi\cdot k\cdot j\cdot\iota}{2^m}} |k\rangle. \tag{1}$$

A Transformada Quântica de Fourier é uma operação unitária, inversível e de tempo polinomial em relação ao tamanho da entrada. Além do algoritmo quântico de fatoração, outras aplicações da QFT compreendem a quebra da imprevisibilidade de geradores pseudo-aleatórios criptograficamente seguros [5], o cálculo da síndrome para decodificação de códigos grafos quânticos [6], dentre outras.

Embora a QFT possua importância para a Computação e para as Comunicações, ainda não existe um computador quântico de larga escala capaz de implementá-la, a maioria das implementações é de poucos qubits e possui caráter experimental [7]. Além disso, há limitações intrínsecas na simulação de um computador quântico por um computador clássico [8]. Levando em consideração tais dificuldades, neste trabalho será apresentada uma ferramenta para simulação da QFT em computadores clássicos, denominada *FTSimulator*.

Para apresentar a ferramenta mencionada, o presente artigo está organizado como segue. A descrição do *FTSimulator* é apresentada na Seção II. A avaliação da ferramenta proposta, em termos do tempo de execução e do número máximo de qubits simuláveis, é feita na Seção III. Por fim, as considerações finais e os trabalhos futuros são apresentados na Seção IV.

II. FTSimulator – Um Simulador para a Transformada Quântica de Fourier

A simulação da Transformada Quântica de Fourier no contexto do *FTSimulator* é realizada sob a forma de *emulação*, na qual um computador clássico executa algoritmos que aproximam o funcionamento deste de um computador quântico [9].

A entrada para a QFT é uma *matriz densidade*. Este tipo de entrada foi escolhido por permitir representar estados quânticos de forma mais genérica o possível, incluindo estados puros (equivalente aos estados de um computador clássico) até estados altamente emaranhados [4].

Para exemplificar o funcionamento do *FTSimulator* ao executar a transformada Quântica de Fourier, suponha que o estado de Bell $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ seja fornecido como entrada via o arquivo `input_qft.txt` contendo a matriz ilustrada na Eq. (2).

$$\rho_{\text{input}} = \begin{bmatrix} 0,5 & 0 & 0 & 0,5 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0,5 & 0 & 0 & 0,5 \end{bmatrix} \tag{2}$$

Vale salientar que este estado quântico de dois qubits é um estado emaranhado e superposto, ilustrando duas características intrinsecamente quânticas. O *FTSimulator* efetua o seguinte processamento: $\rho_{\text{output}} = \mathrm{QFT}\,\rho_{\text{input}}\,\mathrm{QFT}^{\dagger}$, em que o operador QFT é obtido conforme descrito em [4, Cap. 5]. Como resultado, a matriz densidade ρ_{output}, apresentada na Eq. (3), é armazenada no arquivo `output_qft.txt`.

$$\rho_{\text{output}} = \begin{bmatrix} 0,5 & 0,25+0,25\iota & 0 & 0,25-0,25\iota \\ 0,25-0,25\iota & 0,25 & 0 & -0,25\iota \\ 0 & 0 & 0 & 0 \\ 0,25+0,25\iota & 0,25\iota & 0 & 0,25 \end{bmatrix} \tag{3}$$

Francisco R. F. Pereira, Elloá B. Guedes, e Francisco M. de Assis, Instituto de Estudos em Computação e Informação Quânticas (IQuanta), Universidade Federal de Campina Grande, Av. Aprígio Veloso, 882 – Campina Grande-PB – Brazil, E-mails: {revson.ee, elloaguedes, fmarassis}@gmail.com. Os autores agradecem ao CNPQ, CAPES e ao projeto QUANTA/RENASIC/FINEP.

A saída da QFT no FTSimulator consiste em um arquivo contendo a matriz densidade resultante da transformada.

Em virtude da possibilidade de uma explosão exponencial de estados, nem todo tamanho de entrada pode ser processado por um determinado *hardware*, especialmente devido às limitações em termos de quantidade de memória principal. Na tentativa de estimar qual o tamanho máximo de entrada processável por uma determinada configuração de hardware, foi feita uma avaliação do *FTSimulator*, a qual é apresentada na seção a seguir.

III. Avaliação do Simulador

Para avaliar o *FTSimulator* em termos da transformada quântica de Fourier foi necessário o desenvolvimento de dois módulos adicionais: (1) um *módulo para geração de matrizes de operadores densidade*, respeitando as propriedades de que tais operadores são hermitianos, positivos e possuem traço igual a 1; e (2) um *módulo de controle de testes*, o qual recebe como entrada a ordem n das matrizes dos operadores densidade que devem ser geradas e o número de repetições r necessárias para atingir um certo nível de significância estatística. Este último módulo mencionado é responsável por invocar o módulo para geração de matrizes de operadores densidade e o *FTSimulator*, produzindo ao final um relatório contendo a ordem das matrizes e o tempo de execução que o *FTSimulator* demandou para realizar a transformada Quântica de Fourier sobre cada uma delas. A organização de tais módulos e a relação do fluxo de dados são ilustrados na Figura 1.

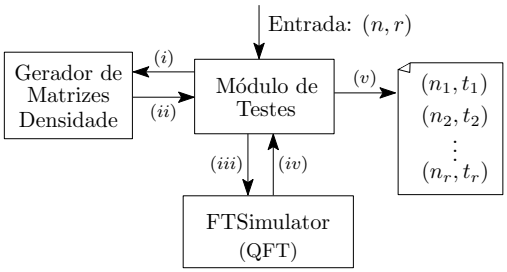

Fig. 1. Idéia geral do processo de avaliação do tempo de execução para a transformada quântica de Fourier

Após fixar um valor de n e executar um número pequeno de repetições com o intuito de estimar a média e o desvio padrão no tempo de execução da QFT no *FTSimulator* para operadores densidade com esta ordem, foi escolhido um nível de confiança de 95% para geração das estatísticas. Levando em consideração estes dados e seguindo procedimentos para estudos experimentais, tal como reportado em Lilja [9], foi possível estabelecer o número necessário de repetições r para assegurar a significância estatística.

Com alguns valores de n e r, foi possível, então, avaliar o *FTSimulator* de acordo com os passos ilustrados na Figura 1: (i) o módulo de testes solicita ao módulo gerador de matrizes densidade um operador de ordem n; (ii) o operador é gerado com o auxílio de um gerador pseudo-aleatório, suas propriedades são checadas e o operador é devolvido ao módulo de testes; (iii) o módulo de testes passa o operador obtido para o *FTSimulator* e inicia um temporizador; (iv) o *FTSimulator* retorna a transformada quântica de Fourier do operador fornecido e o temporizador é parado; (v) o módulo de testes armazena o valor de n e o intervalo de tempo t do temporizador em um arquivo. O temporizador é zerado e o processo é repetido $r - 1$ vezes.

Utilizando um desktop bi-nucleado com clock de 3 GHz e memória principal de 2 GB, foi possível obter os seguintes dados, para $n = 2^m$ com $m = 2, \ldots, 10$, como mostrado na Figura 2. Os dados desta figura mostram que os intervalos de confinça possuem um desvio-padrão baixo e que o tempo necessário para a execução da QFT pelo *FTSimulator* para as entradas fornecidas é da ordem de segundos. Considerando a configuração de *hardware* mencionada, o limite máximo para o tamanho da entrada foi de 10 qubits. Em posse de tais dados, é possível concluir que o *FTSimulator* executa corretamente a QFT em um tempo aceitável para entradas de tamanho razoável, as quais podem ser melhoradas aumentando particularmente a memória principal do *hardware* disponível.

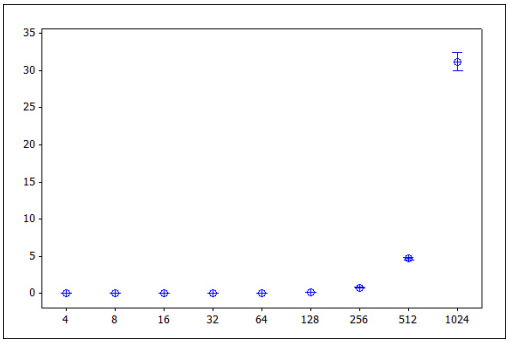

Fig. 2. Intervalos de confiança para o tempo de execução (eixo y) da QFT em função da ordem dos operadores densidade fornecidos como entrada (eixo x).

IV. Considerações Finais

Este artigo apresentou uma ferramenta chamada *FTSimulator*, de código aberto e desenvolvida em âmbito acadêmico, para simulação da transformada quântica de Fourier. Dada a importância desta transformada no contexto da Computação e Informação Quântica, acredita-se que esta ferramenta possa ser de grande utilidade no ensino-aprendizagem desta transformada e também possa servir de suporte em pesquisas. O repositório do FTSimulator pode ser acessado em `http://ftsimulator.googlecode.com`.

Em pesquisas futuras, almeja-se executar a ferramenta em outras configurações de *hardware*, com o intuito de obter um comparativo para os tempos de execução obtidos, além de tentar aumentar o número de qubits executáveis. Uma outra linha de investigação que está sendo considerada é a utilização do *FTSimulator* como componente da simulação do algoritmo quântico da fatoração [2].

Referências

[1] S. Imre and F. Balazs, *Quantum Computing and Communications - An Engineering Approach*, J. W. . Sons, Ed. John Wiley & Sons, 2005.
[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.
[3] J. A. Gregg, "On factoring integers and evaluating discrete logarithms," Master's thesis, Harvard College, 2003.
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
[5] E. B. Guedes, F. M. de Assis, and B. Lula Jr., "Quantum attacks on pseudorandom generators," *Mathematical Structures in Computer Science*, vol. 23, pp. 1–27, 2013.
[6] G. O. Santos, F. M. de Assis, and A. F. de Lima, "Explicit error syndrome calculation for quantum graph codes," *Quantum Information Processing*, vol. 12, no. 2, pp. 1269–1285, 2013.
[7] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, pp. 45–53, 2010.
[8] R. Feynman, "Simulating Physics with Computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, 1982.
[9] D. Lilja, *Measuring Computer Performance*, C. U. Press, Ed. Cambridge University Press, 2004.