Proposta de Trabalho de Formatura

Computação Quântica: Complexidade e Algoritmos

Aluno: Carlos Henrique Cardonha
Orientadora: Cristina Gomes Fernandes

Esta proposta consiste num trabalho de iniciação científica, financiado pela FAPESP n.03/13236-0.

1 Introdução

Pode-se dizer que a teoria de computação quântica iniciou-se nos anos 80, quando Feynman [4] observou que um sistema quântico de partículas, ao contrário de um sistema clássico, parece não poder ser simulado eficientemente em um computador clássico e sugeriu um computador que explorasse efeitos da física quântica para contornar o problema.

Desde então, até 1994, a teoria de computação quântica desenvolveu-se discretamente, com várias contribuições de Deutsch [2, 3], Bernstein e Vazirani [1], entre outros, que colaboraram fundamentalmente para a formalização de um modelo computacional quântico.

Foi apenas em 1994 que a teoria recebeu um forte impulso e uma enorme divulgação. Isso deveu-se ao algoritmo de Shor [9, 10], um algoritmo quântico para fatoração de inteiros, considerado o primeiro algoritmo quântico combinando relevância prática e eficiência. O algoritmo de Shor é uma evidência de que o modelo computacional quântico proposto pode superar de fato o modelo clássico. Dado um inteiro n com pelo menos dois divisores primos distintos, o algoritmo de Shor calcula um divisor não-trivial de n em tempo $O(\log^3 n)$. O problema da fatoração de inteiros é reconhecidamente difícil do ponto de vista clássico, a ponto de ser a base de um dos mais famosos sistemas criptográficos atualmente em uso, o RSA [8]. O resultado de Shor impulsionou tanto a pesquisa prática, objetivando a construção de um computador segundo o modelo quântico, quanto a busca por algoritmos criptográficos alternativos e algoritmos quânticos eficientes para outros problemas difíceis. Essas e várias outras questões, relacionadas tanto com a viabilidade do modelo quântico quanto às suas limitações, têm sido objeto de intensa pesquisa científica.

2 Objetivos

Estudar os fundamentos da teoria de computação quântica. Este trata-se de um projeto conjunto de iniciação científica envolvendo o aluno Carlos Henrique Cardonha e o aluno Marcel Kenji de Carli Silva.

Inicialmente visamos complementar o estudo das áreas afins ligadas ao tema e posteriormente nos aprofundar nos aspectos de teoria de complexidade computacional e nos aspectos algorítmicos desta nova área.

Das áreas afins, estudaremos os seguintes tópicos, que são necessários para o entendimento do modelo e de suas potencialidades: espaços de Hilbert, fundamentos de mecânica quântica, modelos de computação clássicos (máquinas de Turing, determinísticas e probabilísticas, circuitos booleanos) e outros que se mostrem necessários a medida que avançamos nos estudos.

No que diz respeito a computação quântica propriamente, concentraremos os nossos estudos em dois tópicos da teoria de computação quântica: complexidade computacional (o estudo do novo modelo propriamente, de circuitos quânticos, universalidade, classes de complexidade advindas do modelo quântico, etc) e algoritmos quânticos (o estudo dos algoritmos de Deutsch, de Simon, de Shor e de Grover).

Como subproduto da iniciação científica, pretendemos produzir um texto, nos moldes do que está sendo produzido já (`http://www.linux.ime.usp.br/~magal/quantum/`), com todo o conteúdo que for estudado durante esta iniciação científica.

Durante os três primeiros meses do projeto, os dois alunos estudaram os mesmos temas, por se tratarem de tópicos básicos da disciplina. A partir do quarto mês, o Carlos começou a se concentrar no estudo dos aspectos de complexidade computacional, enquanto o Marcel começou a se concentrar no estudo dos algoritmos de Shor e de Grover.

3 Atividades realizadas

Os resultados concretos do estudo realizado até o momento encontram-se no texto que está sendo produzido. A seguir, contamos como foi feito o estudo durante o período do relatório, que itens da bibliografia foram estudados, os progressos e as dificuldades encontrados durante o estudo feito. Terminamos com um cronograma de estudos.

Nos primeiros meses do ano, terminamos de ler o artigo de Rieffel e Polak [7]. Esse artigo serviu para revisão dos assuntos estudados durante o ano passado. Entre esses assuntos, podemos destacar o estudo das bases de Hilbert e da sobreposição de estados no universo quântico. O artigo também foi interessante por mostrar possíveis aplicações da computação quântica em áreas tradicionais da computação, como a criptografia.

No início do projeto, estudei no livro de Feynman [5] alguns conceitos relacionados às portas lógicas. O objetivo inicial era entender como funcionam os circuitos lógicos na computação quântica, pois como a parte de complexidade envolve a medição do consumo de tempo dos algoritmos, gostaríamos de saber a relação que existe entre os circuitos quânticos e o consumo de tempo dos algoritmos quânticos.

O que foi lido basicamente serviu para mostrar determinadas portas baseadas no modelo físico-quântico, como as portas universais de Toffoli e Fredkin, mas não foi suficiente para mostrar como funcionariam essas portas num computador quântico, especialmente a contagem de tempo. Como não conseguimos entender exatamente como funcionam os circuitos lógicos no modelo quântico, preferimos não escrever nada no texto até encontrarmos algum material que esclareça esse ponto.

Após duas semanas estudando os circuitos lógicos, decidimos estudar todo o artigo de Vazirani e Berstein [1]. O artigo é longo e técnico, e consumiu por volta de dois meses de leitura, entremeada pela consulta a vários outros artigos. Basicamente, os autores mostram nesse artigo uma série de resultados para no final construir uma máquina de Turing quântica universal.

Uma série de peculiaridades que aparecem na computação quântica acabam por criar dificuldades não encontradas no modelo clássico. Isso acabou implicando na especificação de uma série de definições e construções de formas pouco convencionais, e nem sempre os autores deixavam claro o porquê de suas escolhas. Essas omissões resultavam sempre em um consumo considerável de tempo para a compreensão do que estava sendo feito.

Outra questão importante diz respeito a medição de tempo. Inicialmente, pensamos que o artigo ia cobrir a maioria das questões relevantes para o estudo de complexidade para o modelo quântico de computação. Porém, os autores não fazem qualquer comentário a respeito dos circuitos e das portas lógicas, e as dúvidas que tínhamos antes do início da leitura do artigo não foram resolvidas.

Os primeiros resultados apresentados no artigo envolviam conceitos razoavelmente conhecidos. Durante a leitura dessa parte inicial, aproveitamos para rever alguns conceitos vistos desde o início de nossos estudos. A parte na qual nos concentramos, porém, envolvia a decomposição de matrizes unitárias de dimensão arbitrária em matrizes unitárias denominadas *quase-triviais*. Tais decomposições são descritas levando em conta erros numéricos, advindos de cálculos envolvendo números reais e eventuais imprecisões na execução de operações quânticas na prática.

Durante a leitura desse artigo, a consideração dos erros durante as computações acabou dificultando a compreensão do texto. Os autores não deixaram muito claro as relações que existem entre os diversos erros que são considerados durante o texto, e isso acabava confundindo, pois não sabíamos direito quando um erro que estava sendo discutido num determinado momento era consequência de outro já citado ou era intrínseco ao resultado apresentado.

Com a finalidade de compreender melhor a natureza dos resultados ali apresentados, decidimos separar a parte que leva em conta os erros dos resultados de decomposição das matrizes unitárias. Para tanto, os resultados principais de Bernstein e Vazirani foram reescritos sob outra forma e são apresentados de uma maneira bem mais simplificada no nosso texto. Os resultados que apresentamos porém, acreditamos, preservam a essência da idéia, e ainda servem para elaborar a máquina de Turing quântica universal (sem levar em conta os erros de precisão).

Apesar de considerar uma versão simplificada dos resultados do artigo, gastamos bastante tempo escrevendo sobre essas decomposições, pois nosso objetivo foi deixar tudo o mais claro possível. Para isso, expandimos as discussões feitas pelos autores nas partes que consideramos mais obscuras e difíceis.

Mais recentemente, motivados pelo que foi visto durante esse semestre na disciplina de Complexidade Computacional (MAC430), que estamos cursando, resolvi revisar e expandir a parte inicial do texto, onde eram apresentados os modelos de computação.

A versão que tínhamos dessa parte foi transformada numa introdução e pretendemos incluir na parte dos modelos a descrição da máquina de Turing universal para o modelo clássico. Foram incluídas as definições de máquina de Turing não-determinística e das principais classes de complexidade clássicas.

4 Cronograma revisado

O cronograma estipulado para os próximos 6 meses é o seguinte.

Ativ/Mês	5	6	7	8	9	10
1	$\surd$					
2	$\surd$					
3		$\surd$	$\surd$			
4			$\surd$	$\surd$		
5				$\surd$	$\surd$	
6						$\surd$

Legenda:
1. Estudo das notas de aula de Preskill [6].
2. Reescrita e término dos capítulos de modelos clássicos de computação.
3. Estudo das classes quânticas de computação e sua relação com as classes clássicas no capítulo do modelo quântico de computação.
4. Complementação do estudo de circuitos lógicos quânticos.
5. Estudo da relação entre circuitos lógicos quânticos, máquinas de Turing quânticas e os algoritmos quânticos da literatura, com especial ênfase na medida de tempo.
6. Finalização do texto e preparação do relatório final.

5 Estrutura da monografia

A monografia será constituída do texto que já está sendo preparado, apresentando a área de computação quântica. Pretendemos que seja, dentro do possível, um texto que possa ser lido e compreendido por qualquer pessoa com uma formação razoável em ciência da computação e que passe a idéia do que consiste o modelo quântico de computação, quais as principais diferenças em relação ao modelo clássico, exemplos de algoritmos quânticos, incluindo o mais famoso deles, de Shor, para fatoração de inteiros, e incluindo também a apresentação das classes de complexidade quânticas e suas relações com as clássicas. Parte desse texto já está escrita, e está acessível no endereço `http://www.linux.ime.usp.br/~magal/quantum/quantum.ps`.

Referências

[1] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5):1411–1473, 1997.

[2] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Roy. Soc. London Ser. A*, 400(1818):97–117, 1985.

[3] D. Deutsch. Quantum computational networks. *Proc. Roy. Soc. London Ser. A*, 425(1868):73–90, 1989.

[4] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6 & 7):467–488, 1982.

[5] R. Feynman. *Feynman Lectures in Computation.* Addison Wesley, 1996.

[6] J. Preskill. *Lecture Notes for Physics 219/Computer Science 219.* Disponível em http://www.theory.caltech.edu/people/preskill/ph229.

[7] E. Rieffel and W. Polak. Introduction to quantum computing. *ACM Computing Surveys*, 32(3):300–335, 2000.

[8] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[9] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124–134. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

[10] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.