Proposta de Trabalho de Formatura

Computação Quântica: Complexidade e Algoritmos

Aluno: Marcel Kenji de Carli Silva
Orientadora: Cristina Gomes Fernandes

Esta proposta consiste num trabalho de iniciação científica
financiado pela FAPESP (processo no. 03/13237-7).

1 Introdução

Pode-se dizer que a teoria de computação quântica iniciou-se nos anos 80, quando Feynman [10] 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 [7, 8], Bernstein e Vazirani [3], 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 [19, 20], 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 [17]. 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 os alunos Marcel Kenji de Carli Silva e Carlos Henrique Cardonha.

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 Marcel começou a se concentrar no estudo dos algoritmos de Shor e de Grover, enquanto o Carlos começou a se concentrar no estudo dos aspectos de complexidade computacional.

3 Atividades realizadas

Os resultados concretos do estudo realizado até o momento encontram-se no texto que está sendo produzido, que segue em anexo. 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.

Inicialmente estudei por cerca de duas semanas, seguindo o livro de Grus-

ka [12], os conceitos de registrador quântico, teorema do no-cloning e emaranhamento quântico (*quantum entanglement*), essenciais para o prosseguimento do projeto. O teorema do no-cloning mostra limitações fundamentais impostas pelo fato de que as operações sobre registradores precisam ser unitárias. O fenômeno do emaranhamento quântico mostra porque não é trivial simularmos eficientemente um computador quântico através de um computador no modelo clássico. (Na verdade, não se sabe até hoje se tal simulação eficiente é possível.)

Feito isso, começamos um estudo aprofundado do artigo de Bernstein e Vazirani [3] sobre complexidade no modelo quântico. O texto é bem extenso e levamos cerca de quatro semanas para ler todo o conteúdo. Os autores definem uma máquina de Turing quântica e as operações permitidas. Depois algumas limitações, como reversibilidade e necessidade de sincronização, são tratadas com mais cuidado, pois elas dificultam a implementação de primitivas que são fáceis de se usar no modelo clássico, como laços e condicionais.

É apresentada então uma série de resultados sobre decomposição de matrizes unitárias de dimensão arbitrária em matrizes unitárias de dimensão 2 definidas como *quase-triviais*, que são as rotações e mudanças de fase. Esta seção nos interessou muito e estudamos o assunto a fundo. Porém, tivemos algumas dificuldades de compreensão pois os autores não deixaram clara a separação entre os diversos tipos de erros numéricos que podem ocorrer: um deles é pelo fato de que é preciso representar números com uma precisão finita e o outro é pelo fato de utilizarmos rotação e mudança de fase de um único ângulo para aproximar tais operações em ângulos arbitrários.

Finalmente, os resultados de todas as seções anteriores são sintetizados para a construção de uma máquina de Turing universal quântica. Ao longo do texto, diversas vezes é discutido o aspecto de erros de arredondamento e porque uma máquina quântica não é considerada uma máquina analógica. Tais discussões tinham menos relevância para nosso estudo, de modo que não nos detivemos nesses detalhes onde julgamos adequado. No nosso texto, optamos por apresentar uma versão dos resultados de decomposição de Bernstein e Vazirani [3] omitindo-se os erros advindos da impossibilidade de se manipular números com precisão infinita.

Cabe ressaltar que a nossa compreensão do artigo foi facilitada pelo fato de estarmos cursando neste primeiro semestre a disciplina MAC0430 Algoritmos e Complexidade de Computação, através da qual nos familiarizamos com diversos conceitos relevantes.

Esperávamos encontrar neste artigo uma formulação precisa da medida

de tempo no modelo quântico. Como o que foi encontrado não é claramente equivalente ao que foi encontrado em outras fontes, onde a análise de tempo é feita em função da profundidade ou tamanho de circuitos, resolvemos pesquisar mais sobre o assunto. Procuramos então por tal formulação no livro de Gruska [12] e nos artigos de Barenco et al. [2, 1], Shor [20] e Deutsch et al. [9], mas nada definitivo foi encontrado. Após duas semanas de discussão chegamos a uma formulação razoável do ponto de vista matemático, mas que não sabemos se é realístico fisicamente.

O que buscamos é algum tipo de resultado de decomposição de matrizes unitárias em matrizes unitárias "pequenas", que correspondam às operações básicas realizáveis em um computador quântico. O que não é muito claro é quais matrizes unitárias seriam os blocos básicos de uma tal decomposição.

O estudo do artigo de Bernstein e Vazirani [3] nos levou a postergar o estudo do papel dos circuitos quânticos nesse contexto. Com o estudo de tais circuitos e sua relação com o modelo de computação adotado — a máquina de Turing quântica — acreditamos que tais dúvidas deverão ser resolvidas. É nosso plano fazer esse estudo em julho através das notas de aula de Preskill [16].

Enquanto o Carlos trabalhava em reescrever os resultados de decomposição de matrizes unitárias de Bernstein e Vazirani [3], iniciei o estudo dos problemas de Deutsch e de Deutsch-Jozsa e dos algoritmos quânticos que os resolvem. Isso foi feito através do livro de Gruska [12] e do artigo de Cleve et al. [5], que apresenta versões melhoradas dos algoritmos propostos originalmente. O problema de Deustch-Jozsa não pode ser resolvido eficientemente no modelo clássico, mas isso é possível no modelo probabilístico. Alguns conceitos básicos de algoritmos e classes de complexidade probabilísticos foram estudados no livro de Papadimitriou [15]. Isso durou cerca de duas semanas.

Passamos então para o problema de Simon [21], durante duas semanas. Estudamos o algoritmo que resolve o problema. Para a análise de sua correção e do tempo esperado, precisamos utilizar alguns conceitos de álgebra linear acerca de espaços vetoriais definidos sobre corpos finitos. Tais conceitos foram estudados através do livro de Moreira e Kohayakawa [13].

Como pré-requisito para o estudo do algoritmo de fatoração de Shor, começamos o estudo de alguns testes probabilísticos de primalidade. Antes de entrar na parte de teoria dos números propriamente dita, estudamos mais cuidadosamente sobre algoritmos e classes de complexidade probabilísticos, através dos livros de Papadimitriou [15] e de Motwani e Raghavan [14].

Estudamos um pouco de teoria dos números tanto para a familiarização com os conceitos e certas propriedades como também pelo fato de eles serem essenciais para a compreensão de testes de primalidade e do algoritmo de Shor. Esse estudo foi feito através do livro de Papadimitriou [15], de Knuth, Graham e Patashnik [11] e de Rosen [18]. O teste de primalidade de Miller-Rabin foi estudado através do famoso livro de Cormen et al. [6].

Por fim, sondamos quais aspectos da transformada de Fourier deveriam ser estudados para a compreensão da transformada quântica de Fourier e seu uso no algoritmo de fatoração de Shor. A teoria sobre tais transformadas é bastante extensa e pretendemos estudar a fundo apenas resultados relevantes para nosso projeto. Alguns progressos foram obtidos através da leitura do livro de Gruska [12], Brigham [4] e Cormen et al. [6].

Vale ressaltarmos que, ao longo deste período, revisamos constantemente diversas seções do nosso texto, aprimorando-as. Não conseguimos ainda escrever sobre todos os assuntos estudados, mas pretendemos fazê-lo ao longo do período seguinte.

4 Cronograma para o próximo período

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

Ativ/Mês	5	6	7	8	9	10
1	√					
2	√					
3		√				
4		√	√	√		
5				√	√	
6						√

Legenda:
1. Estudo (de parte) das notas de aula de Preskill [16].
2. Inclusão no texto da parte estudada sobre algoritmos para teste de primalidade no modelo clássico.
3. Estudo da transformada de Fourier quântica.
4. Estudo dos algoritmos de Shor.
5. Estudo dos algoritmos de Grover.
6. Finalização do texto e preparação do relatório final.

O estudo da parte das notas de aula de Preskill [16] tem como objetivo identificar a relação entre a medida de consumo de tempo numa máquina de Turing quântica, num circuito quântico e nos algoritmos quânticos descritos na literatura. O estudo da transformada de Fourier quântica será voltada a entendermos seu papel nos algoritmos quânticos. Os itens 3, 4 e 5 incluem a escrita do material referente a esses tópicos.

Considerando que, durante o próximo semestre, estaremos cursando menos disciplinas e metade delas são disciplinas mais leves, acreditamos que o cronograma acima é viável e deixa espaço para possíveis revisões do texto que se mostrem necessárias.

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 sua relação 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] A. Barenco. A universal two-bit gate for quantum computation. *Proc. Roy. Soc. London Ser. A*, 449(1937):679–683, 1995.

[2] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N.H. Margolus, P.W. Shor, T. Sleator, J.A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, 1995.

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

[4] E.O. Brigham. *The fast Fourier transform*. Prentice-Hall, Englewood Cliffs, New Jersey, 1974.

[5] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci.*, 454(1969):339–354, 1998.

[6] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein. *Introduction to algorithms*. MIT Press, Cambridge, MA, second edition, 2001.

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

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

[9] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. *Proc. Roy. Soc. London Ser. A*, 449(1937):669–677, 1995.

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

[11] R.L. Graham, D.E. Knuth, and O. Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994. A foundation for computer science.

[12] J. Gruska. *Quantum computing*. Advanced Topics in Computer Science Series. McGraw-Hill International (UK) Limited, London, 1999.

[13] C.G. Moreira and Y. Kohayakawa. *Tópicos em combinatória contemporânea*. Publicações Matemáticas do IMPA. Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2001. 23º Colóquio Brasileiro de Matemática.

[14] R. Motwani and P. Raghavan. *Randomized algorithms*. Cambridge University Press, Cambridge, 1995.

[15] C.H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994.

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

[17] 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.

[18] K.H. Rosen. *Elementary number theory and its applications*. Addison-Wesley, Reading, MA, fourth edition, 2000.

[19] 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.

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

[21] D.R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997.