ISSN: 2526-1371

Uma Revisão sobre a Relação de BQP com outras Classes de Complexidade Computacional

Henrique Hepp[1], **Murilo V. G. da Silva**[1], **Leandro M. Zatesko**[2]

[1]Departamento de Informática, Universidade Federal do Paraná

[2]Departamento de Informática, Universidade Tecnológica Federal do Paraná

{hhepp,murilo}@inf.ufpr.br, zatesko@utfpr.edu.br

Abstract. *The class of problems for which there are efficient quantum algorithms, denoted by* BQP *(Bounded-error Quantum Polynomial), is still not well understood. A common approach in theoretical computer science for understanding the limits of a class of complexity is to clarify its relations with other classes. This article presents a brief survey of the relations of* BQP *with the most known classical and quantum complexity classes.*

Resumo. *A classe de problemas para os quais existem algoritmos quânticos eficientes, denotada por* BQP *(Bounded-error Quantum Polynomial), ainda é pouco compreendida. Uma abordagem comum em teoria da computação para a compreensão dos limites de uma classe de complexidade é esclarecer relações desta com outras classes. Este artigo apresenta um breve survey das relações de* BQP *com as classes de complexidade computacional clássicas e quânticas mais conhecidas.*

Keywords: Quantum Computation; Computational Complexity; BQP; BPP

Palavras-chave: Computação Quântica; Complexidade Computacional; BQP; BPP

1. Introdução

Os modelos clássico e quântico de computação definem duas classes diferentes de problemas computacionais que podem ser resolvidos em tempo polinomial. Em computação clássica, denotamos tal classe por P e em computação quântica por BQP, ou *Bounded-error Quantum Polynomial*.

Em computação clássica, uma outra classe importante é a classe dos problemas decididos em tempo polinomial por algoritmos aleatorizados, denominada BPP, *Bounded-error Probabilistic Polynomial time*, que claramente generaliza P. A classe BPP está contida na classe BQP, por outro lado, acredita-se que a classe BQP não seja igual à classe BPP, pois existem algoritmos polinomiais quânticos para problemas que conjecturam-se não estar em BPP, como por exemplo, o algoritmo de Shor, que resolve o problema de fatoração em números primos.

Classes de complexidade que contêm BQP têm sido alvo recente de investigação em diversos trabalhos [Aaronson 2005, Aaronson et al. 2016,

Morimae and Nishimura 2017]. Pois os estudos de classes mais poderosas que BQP ajudam a compreender a estrutura matemática de diversos problemas computacionais, em particular, problemas na fronteira entre o que pode e o que não pode ser revolvido por algoritmos quânticos de maneira eficiente.

Nessa revisão apresentamos as classes de complexidade mais relevantes no contexto de computação quântica e suas relações com a classe BQP. O artigo está organizado da seguinte maneira. A Seção 2 apresenta uma introdução às classes de complexidade quântica. A Seção 3 apresenta as principais classes de complexidade relacionadas com BQP e a Seção 4 conclui o artigo.

2. Classes de Complexidade Quânticas

Nesse artigo assumimos que o leitor tenha familiaridade com classes de complexidade computacional em geral. Para maiores detalhes indicamos o livro [Arora and Barak 2009]. Nessa seção apresentamos apenas os preliminares matemáticos para definição das classes de complexidade quânticas. Para maiores detalhes sobre o modelo de computação quântica indicamos o livro [Nielsen and Chuang 2011].

O estado de um sistema quântico é um vetor unitário de números complexos chamado de *vetor de estado* representado por $|\psi\rangle$. De modo geral, um vetor de estado $|\psi\rangle$ em um espaço com N dimensões $\mathbb{C}^N$ pode ser descrito pela combinação linear de N estados linearmente independentes: $|\psi\rangle = \alpha_1 |1\rangle + \alpha_2 |2\rangle + \alpha_3 |3\rangle + \cdots + \alpha_N |N\rangle$, onde $\alpha_1, \cdots \alpha_N$ são números complexos. Como $|\psi\rangle$ é um vetor unitário, temos que $\sum_i |\alpha_i|^2 = 1$.

Para a computação quântica usa-se o vetor de estado mais simples, que é o *qubit*, uma generalização do bit. Enquanto o bit pode ser representado por $\{0, 1\}$, o qubit é um estado quântico $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, onde $\alpha, \beta \in \mathbb{C}$ e $|\alpha|^2 + |\beta|^2 = 1$. De forma mais geral, o estado quântico que descreve n qubits é produto tensorial entre os n qubits $|i\rangle$, dado por $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ onde $\alpha_0, \cdots, \alpha_{2^n-1} \in \mathbb{C}$ e $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$.

Transformações Unitárias são transformações dos estados quânticos de modo que eles continuem sendo vetores unitários. Em outras palavras, seja U uma transformação unitária, $|\Psi'\rangle = U |\Psi\rangle$. Uma *porta quântica* que age sobre qubits é uma transformação unitária agindo sobre o vetor correspondente aos qubits em questão.

Dado o estado $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$, podemos fazer uma *medição quântica* de $|\Psi\rangle$ com relação à base $\{|0\rangle, |1\rangle, \cdots, |2^n - 1\rangle\}$. Ao fazermos a medição obtemos um dos estados $|i\rangle$ com probabilidade $|\alpha_i|^2$ e perdemos todas as informações do estado original. Em outras palavras, ao se medir $|\Psi\rangle$, o estado *colapsa* em $|i\rangle$ com probabilidade $|\alpha_i|^2$.

Um *circuito quântico* é um grafo direcionado acíclico onde cada vértice pode ser uma porta quântica ou uma medição agindo sobre qubits. O tamanho do circuito é o número de vértices do grafo. Um *algoritmo quântico* é uma família infinita de circuitos quânticos $\{C_n\}, n \in \mathbb{N}^*$, sendo que deve ser possível obter a descrição de C_n por meio de uma maquina de Turing de tempo polinomial em n.

A classe BQP, ou *Bounded-error Quantum Polynomial Time*, é a classe de problemas de decisão resolvidos por uma família uniforme de circuitos quânticos com tamanho polinomial. Isto é, uma instância positiva é aceita com probabilidade pelo menos maior

ou igual a $2/3$, uma instância negativa é aceita com probabilidade menor que $1/3$. Chamamos os problemas dessa classe por problemas que admitem um algoritmo BQP.

A classe QMA, ou *Quantum Merlin-Arthur*, é a classe de problemas cujas instâncias verdadeiras admitem certificados quânticos (i.e., estados quânticos) que podem ser verificadas em tempo polinomial quântico. Ou seja, QMA se relaciona com BQP assim como NP se relaciona com P (assim como MA com relação à BPP, quando permitimos aleatoriedade).

A classe CQP, ou *Collapse-free Quantum Polynomial Time*, é a classe de problemas resolvidos por um algoritmo BQP contendo medições que não provoquem o colapso dos estados. A classe naCQP, "non-adaptive Collapse-free Quantum Polynomial Time", é a classe CQP com a restrição de que as operações quânticas independem dos resultados das medições que não colapsam. Essas duas classes não são realizáveis fisicamente, pois admitiriam a possibilidade de sinais mais rápidos do que a velocidade da luz, mas fornecem um ferramental útil no estudo da complexidade computacional [Aaronson et al. 2016].

A classe clássica PP, ou *Probabilistic Polynomial-Time*, é equivalente à classe quântica PostBQP, ou *Postselected Bounded-Error Quantum Polynomial-Time*. PostBQP é a classe de problemas resolvidos por um algoritmo BQP com a funcionalidade extra de se poder *assumir* que a medição um determinado qubit sempre será igual a $|1\rangle$ quando essa probabilidade for diferente de zero [Aaronson 2005].

Em complexidade também é muito comum usar-se classes com um oráculo. Um oráculo é uma espécie de "caixa preta" que retorna uma resposta para qualquer pergunta. Se $\mathcal{A}$ é uma classe de complexidade, $\mathcal{A}^B$ denota a classe dos problemas resolvidos por algoritmos em $\mathcal{A}$ com oráculo para problemas completos de B.

3. Relações de BQP com outras Classes de Complexidade

Nas Seções 3.1 e 3.2 são apresentadas respectivamente as relações conhecidas e conjecturadas de BQP com outras classes de complexidade conforme vistas na Figura 1.

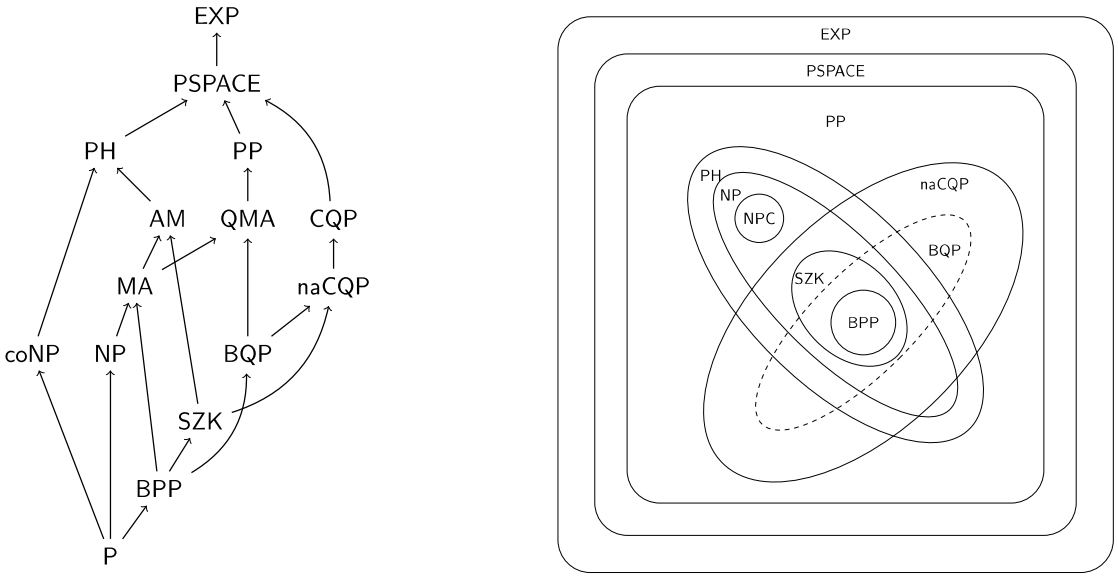
3.1. Relações Conhecidas

Teorema 1. [Gill 1977, Bernstein and Vazirani 1997] $\mathsf{P} \subseteq \mathsf{BPP} \subseteq \mathsf{BQP}$

BPP contém P, pois um algoritmo BPP possui a funcionalidade extra de produzir bits aleatórios. BQP contém BPP, pois além de simular qualquer circuito clássico também tem a habilidade de gerar bits aleatórios usando uma porta quântica chamada de Porta de Hadamard [Nielsen and Chuang 2011].

Teorema 2. [Watrous 2000, Marriott and Watrous 2005] $\mathsf{BQP} \subseteq \mathsf{QMA} \subseteq \mathsf{PP}$

A prova de que BQP está contida em QMA é análoga à prova de que P está contida em NP, generalizando bits para qubits e verificadores polinomiais para verificadores BQP. A classe QMA, por sua vez, está contida em PP. Esse resultado com demonstração bastante técnica foi obtido por Marriott e Watrous. É possível obter-se uma demonstração alternativa usando-se o fato de que $\mathsf{PP} = \mathsf{PostBQP}$ e que QMA é um caso particular de PostBQP [Aaronson 2005].



(a) Relações confirmadas. **(b) Relações conjecturadas.**

Figura 1. Relações entre algumas das principais classes de complexidade.

Teorema 3. [Aaronson et al. 2016] $\mathsf{BQP} \subseteq \mathsf{naCQP} \subseteq \mathsf{CQP} \subseteq \mathsf{PSPACE}$

As duas primeiras inclusões procedem das definições das classes. Para a inclusão de CQP em PSPACE, mostra-se que uma sequência de "queries" para um oráculo que resolva problemas de $\mathsf{BPP}^{\#\mathsf{P}}$ pode ser usado para simular um circuito CQP. A inclusão segue do fato que $\mathsf{BPP}^{\#\mathsf{P}} = \mathsf{BPP}^{\mathsf{PP}} \subseteq \mathsf{PSPACE}$.

Teorema 4. [Goldwasser et al. 1989, Aaronson et al. 2016] $\mathsf{BPP} \subseteq \mathsf{SZK} \subseteq \mathsf{naCQP}$

A classe SZK contém BPP, pois na definição de SZK usa-se um verificador BPP. Para a prova da inclusão de SZK em naCQP usa-se a redução do problema de determinar a diferença estatística de distribuições, completo para SZK.

3.2. Relações Conjecturadas

Conjectura 1. [Aaronson et al. 2016] $\mathsf{NP} \not\subset \mathsf{naCQP}$

No modelo de computação "caixa-preta", provou-se que para encontrar um elemento dentre $2^n = N$ itens, um algoritmo naCQP necessita tempo $\Omega(N^{1/4})$. Isso significa que um algoritmo naCQP não conseguiria resolver por "força-bruta" o problema 3SAT em tempo polinomial, pois no modelo "caixa-preta", a estrutura dos problemas é abstraída. Por isso, acredita-se que a naCQP não contém NP, o que tornaria naCQP apenas um pouco maior que BQP.

Conjectura 2. [Aaronson et al. 2016] $\mathsf{naCQP} \subset \mathsf{PP}$

Considerando-se que (provavelmente) naCQP seja uma classe pouco maior que BQP, suspeita-se que naCQP esteja contido em PP. Atualmente o limite superior conhecido de naCQP é $\mathsf{BPP}^{\mathsf{PP}}$.

Conjectura 3. $\mathsf{SZK} \not\subset \mathsf{BQP}$

Suspeita-se que BQP não contém SZK pois foi encontrado um oráculo A tal que

$\mathsf{SZK}^A \not\subset \mathsf{BQP}^A$ [Aaronson 2002]. Ademais, até então não se encontrou um algoritmo quântico para vários problemas SZK, como o de Isomorfismo de Grafos.

Conjectura 4. $\mathsf{SZK} \subsetneq \mathsf{NP}$

Acredita-se que a SZK seja NP-intermediária, pois a hierarquia polinomial colapsa caso vários problemas importantes em SZK sejam provados como NP-completos [Aiello and Hastad 1991].

Conjectura 5. [Bernstein and Vazirani 1997] $\mathsf{BPP} \subsetneq \mathsf{BQP}$

Acredita-se que a BQP não seja igual à BPP, pois existem algoritmos polinomiais quânticos que conjectura-se não estar em BPP. Tal é o caso do Algoritmo de Shor [Shor 1999] que resolve o problema de fatoração em números primos.

Conjectura 6. $\mathsf{NP} \neq \mathsf{BQP}$. Em particular $\exists L \in \mathsf{NP}$ tal que $L \notin \mathsf{BQP}$ e $\exists L \in \mathsf{BQP}$ tal que $L \notin \mathsf{NP}$.

Acredita-se que BQP não contém NP pelas seguintes razões. Primeiro, até então não se encontrou nenhum algoritmo quântico que resolva um problema NP-completo em tempo polinomial. Segundo, no modelo de computação "caixa-preta", provou-se que para encontrar um elemento dentre $2^n = N$ itens, um algoritmo BQP necessita tempo $\Omega(N^{1/2})$ [Bennett et al. 1997]. Isso significa que um algoritmo BQP não conseguiria resolver por "força-bruta" o problema 3SAT em tempo polinomial.

Também se acredita que NP não contém BQP. Primeiro, porque os problemas BQP-completos conhecidos, até onde se sabe, não estão em NP. Segundo, por que existe um oráculo A tal que $\mathsf{BQP}^A \not\subseteq \mathsf{NP}^A$ [Watrous 2000].

Conjectura 7. $\mathsf{PH} \neq \mathsf{BQP}$. Em particular $\exists L \in \mathsf{PH}$ tal que $L \notin \mathsf{BQP}$ e $\exists L \in \mathsf{BQP}$ tal que $L \notin \mathsf{PH}$.

Essa conjectura é uma generalização da Conjectura 6, pois PH é uma classe que generaliza as classes NP e coNP. Conjectura-se que $\mathsf{BQP} \not\subseteq \mathsf{PH}$ pois encontrou-se recentemente um oráculo A tal que $\mathsf{BQP}^A \not\subseteq \mathsf{BH}^A$ [Raz and Tal 2018].

Conjectura 8. $\mathsf{PH} \subseteq \mathsf{PP}$

De acordo com o Teorema de Toda, $\mathsf{PH} \subseteq \mathsf{BP} \cdot \mathsf{PP}$ [Toda 1991, Toda and Ogiwara 1992], sendo que BP é um operador que adiciona uma aleatorização do mesmo modo como é adicionada de P para BPP, ou seja, $\mathsf{BP} \cdot \mathsf{P} = \mathsf{BPP}$. Assumindo hipóteses de desaleatorização, pode-se mostrar que $\mathsf{PH} \subseteq \mathsf{BP} \cdot \mathsf{PP} = \mathsf{PP}$ [Hitchcock and Pavan 2004].

4. Conclusão

Neste artigo foram vistas algumas das relações comprovadas e conjecturadas entre BQP e outras classes de complexidade, juntamente com uma breve ideia das prova ou das razões para as conjecturas feitas. De modo geral, acredita-se que BQP contém restritamente BPP, não contém NP e resolve problemas fora de PH.

Referências

Aaronson, S. (2002). Quantum lower bound for the collision problem. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 635–642. ACM.

Aaronson, S. (2005). Quantum computing, postselection, and probabilistic polynomial-time. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2063):3473–3482.

Aaronson, S., Bouland, A., Fitzsimons, J., and Lee, M. (2016). The space just above BQP. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, pages 271–280. ACM.

Aiello, W. and Hastad, J. (1991). Statistical zero-knowledge languages can be recognized in two rounds. *Journal of Computer and System Sciences*, 42(3):327–345.

Arora, S. and Barak, B. (2009). *Computational Complexity: a Modern Approach*. Cambridge University Press.

Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. (1997). Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, 26(5):1510–1523.

Bernstein, E. and Vazirani, U. (1997). Quantum complexity theory. *SIAM Journal on computing*, 26(5):1411–1473.

Gill, J. (1977). Computational complexity of probabilistic turing machines. *SIAM Journal on Computing*, 6(4):675–695.

Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186–208.

Hitchcock, J. M. and Pavan, A. (2004). Hardness hypotheses, derandomization, and circuit complexity. In *International Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 336–347. Springer.

Marriott, C. and Watrous, J. (2005). Quantum arthur–merlin games. *Computational Complexity*, 14(2):122–152.

Morimae, T. and Nishimura, H. (2017). Merlinization of complexity classes above BQP. *Quantum Information & Computation*, 17(11-12):959–972.

Nielsen, M. A. and Chuang, I. L. (2011). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition.

Raz, R. and Tal, A. (2018). Oracle separation of BQP and PH. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 25, page 107.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332.

Toda, S. (1991). PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877.

Toda, S. and Ogiwara, M. (1992). Counting classes are at least as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 21(2):316–328.

Watrous, J. (2000). Succinct quantum proofs for properties of finite groups. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 537–546. IEEE.