

## 論文内容の要旨

博士論文題目

On the Power and Limitations of Quantum Computing Models: Quantum Walks  
and Communication Complexity

(量子計算モデルの能力と限界：量子ウォークと通信計算量)

氏 名 Marcos Daniel Villagra

(論文内容の要旨)

(1, 200字程度)

To understand the physical limits of computation it is necessary to shift our classical computer models to ones that take into account physical considerations. The best current theory of physical reality is quantum mechanics, which take us to think on computer models based on it. Quantum computation is the study of the power and limitations of computer models that consider quantum mechanical effects like interference and entanglement. Several of the classical computing models like boolean circuits, Turing machines, etc., can be extended to quantum models of computation. In this research we focus on two particular models: the decision tree complexity and communication complexity.

This research is divided in two parts. First we consider Quantum Walks, a very powerful paradigm for the design and analysis of quantum algorithms. Clear mathematical foundations are still lacking for this paradigm. Hence, as a step toward this objective, the following question is being addressed: *Given a graph, what is the probability that a quantum walk arrives at a given vertex after some number of steps?* This is a very natural question, and for classical random walks it can be answered by different combinatorial arguments. For quantum walks this is a highly non-trivial task. Furthermore,

this was only achieved before for one specific coin operator (Hadamard operator) for walks on the line. Even considering only walks on lines, generalizing these computations to a general  $SU(2)$  coin operator is a complex task. The main contribution of this part is a closed-form formula for the question above for a general symmetric  $SU(2)$  operator for walks on lines. As the second contribution, this thesis presents how some basic properties of the walk can be deduced by means of weak convergence theorems for quantum walks.

The second part of this research considers communication complexity; in particular, quantum nondeterministic multiparty communication. There are three different types of nondeterminism in quantum computation: i) strong, ii) weak with quantum proofs, and iii) weak with classical proofs. This thesis is focused on strong quantum nondeterministic protocols where a correct input is accepted with positive probability, and an incorrect input is rejected with probability 1. By extending the definition proposed by de Wolf to nondeterministic tensor-rank ( $nrank$ ), this thesis shows that for any boolean function  $f$ , when there is no prior shared entanglement, the strong quantum nondeterministic communication complexity 1) is upper-bounded by the logarithm of  $nrank(f)$  in the Number-On-Forehead model; and, 2) in the Number-In-Hand model it is lower-bounded by the logarithm of  $nrank(f)$ . One application is a new lower bound for the generalized inner product function on the Number-In-Hand model. As another application of the main result this thesis shows that when the number of players in the protocol is  $o(\log \log n)$  we have that **NQP** is not included in **BQP** in the Number-On-Forehead model.

(論文審査結果の要旨) (A 4 1 枚 1、200字程度)

量子計算は、ニュートン力学に基づく従来の計算原理(古典計算と呼ばれる)とは異なり、量子力学に基づいて動作するものである。そのため、従来の計算よりも強力な情報処理を実現することが期待されている。しかし、期待される能力を発揮する量子計算機を実現することは、現在の技術では非常に困難だと考えられており、より実現可能な範囲での量子計算の能力を研究することが重要であると言える。本論文は、量子計算資源の使用が制限された状況下における量子情報処理の能力に関する考察を行ったもので、得られた主要な成果は以下のとおりである。

【1】論文の目的は一次元離散時間量子ウォークに関する数学的基礎を確立することである。このため、研究では「各グラフに対してあるステップ数の後に特定の頂点に到着する確率」を求める。量子ウォークにおいてこのような確率の計算は様々な手法を用いて求めることができる可能性があるが、そのどれもが非自明である。実際、既存の研究では特定のコイン演算子(アダマール)のみ結果が知られており、一般の  $SU(2)$  演算子に対しては一次元に限定してもその解析は困難である。論文の主な貢献は、コイン演算子として一般の対称  $SU(2)$  演算子を対象とし、上記の確率をフーリエ解析と漸近的近似法により閉形式で求めたことにある。また、量子ウォークの弱収束定理を用いることで、コイン演算子のパラメータと確率分布の台の関係を求めた。

【2】アルゴリズムのために最も一般的な計算モデルは通信モデルである。この通信モデルは単純にプレイヤーが量子ビット(qubit)とエンタングルメントと他の共有する量子モデルに交換できる。本研究では非決定性通信計算量による上限と下限手法を提案する。量子非決定性通信プロトコルを正の確率で受理すると定義されている。文献を一般化して「nondeterministic tensor rank (nrank)」を用いる新しい上限と下限手法を開発した。この手法で各ブール関数に対して量子非決定性通信計算量の上限と下限を証明した。アプリケーションとして Generalized Inner Product 関数において新しいかつ正確な量子通信計算量の下限を証明した。

以上、本論文は学術上、實際上寄与するところが少なくない。よって、本論文は博士(理学)の学位論文として価値あるものと認める。