論文の内容の要旨

論文題目　Resource-Bounded Quantum Computation
（資源制約下における量子計算モデルの計算能力）

氏　名　ルガル　フランソワ

Quantum computation is a recent computation paradigm based on the laws of quantum mechanics. Several results indicates that this computational model is more powerful than classical computation, the most famous being Shor's polynomial-time quantum algorithm solving integer factoring, a problem for which no polynomial time classical algorithm is known. In this dissertation, we further investigate the power of quantum computation models in the framework of computational complexity. We present three results showing that quantum computation is more resource-efficient than classical computation in the models of, respectively, time-bounded computation, nondeterministic communication complexity and space-bounded online computation.

In the first part of this dissertation we study time-efficient quantum algorithms for a group-theoretical problem called the Hidden Subgroup Problem (HSP), which asks to find a subgroup hidden in a group G. The case of G being an Abelian group is actually a simple generalization of the integer factoring problem and can be solved easily on a quantum computer. However, when G is a non-Abelian group, the problem becomes far more difficult and no general polynomial-time quantum algorithm is known. Among all the instances of non-Abelian HSPs, the HSP over the group called dihedral group has received most attention, mainly due to its relation to interesting lattice problems, but, so far, no polynomial-time quantum algorithm is known for this instance. The motivation of our work is the following: can we solve the HSP over groups "close" to the dihedral groups? To answer this question, we study the HSP over a large class of semi-direct product groups, that includes the dihedral groups, and show a classification of these groups into five classes of fundamental semi-direct product groups. Although the HSP over the class corresponding to the dihedral groups seems difficult, we present a polynomial-time quantum algorithm solving the HSP over all the groups of one of the other four classes. We then extend this algorithm, solving, in polynomial time, the HSP over a larger class of groups.

In the second part of this dissertation, we study space-bounded quantum computation under two structured models: the model of quantum communication complexity and the model of quantum online space complexity. From the principles of quantum mechanics,

it is possible to encode n classical bits using a number of "quantum bits" logarithmic in n. A fundamental question is to understand for which computation tasks this property can be used to perform quantum computation using less work space, or less communication resource than in the classical setting.

We first study this problem in the framework of communication complexity, a model in which quantum computation has been proved to be stronger than classical computation. In this model two players, each possessing his own input, want to collaborate to compute the value of a Boolean function depending of both inputs, using as less communication resource as possible. We consider quantum nondeterministic communication complexity. There are two possible definitions of quantum nondeterminism: quantum strong nondeterminism and quantum weak nondeterminism. Although quantum strong nondeterminism is known to be more powerful than classical nondeterminism, the computational power of quantum weak nondeterminism was unknown before our work. We show the first separation between quantum weakly nondeterministic communication complexity and classical nondeterministic communication complexity for a total function. This result shows that quantum proof checking procedures are more communication-efficient than classical ones.

Our third contribution is the first explicit study of quantum online space complexity. We do not know whether a large scale quantum computer can be constructed or not, but it seems that the most severe problem is the construction of quantum memory. Studying what can be done with a small scale quantum memory is thus of paramount importance. It is known that, for space complexity, quantum Turing machines can achieve at most a quadratic gain over classical Turing machines. We show that, when the computation is online, that is, when the input is given one character at once, the situation changes dramatically: there exist languages that a quantum online Turing machine can accept using exponentially less work space than a classical online Turing machine. More precisely, we introduce a model of online quantum Turing machine, very natural and realistic, in which the classical and the quantum parts of the machine are completely separated. We then present a language that can be accepted by such an online quantum Turing machine using logarithm quantum work space, and prove that any online classical probabilistic Turing machine accepting it must use linear space. This leads to the first exponential separation between quantum and classical online bounded-error space complexity.