論 文 の 内 容 の 要 旨

論文題目　Classical Analysis of Quantum Computation
（古典的手法による量子計算の解析）

氏　名　本多　健太郎

Quantum computation is based on quantum physics and different from classical computation based on classical physics. It has non-classical characteristics such as quantum superposition principle, uncertainty principle, and no-cloning theorem and has been mainly studied by original methodology. However, it does not mean we cannot investigate quantum computation using traditional methods that have been studied in non-quantum area. We believe that quite a lot of methods are useful to investigate quantum computation and it is important to find such methods. When they are found, they will accelerate the research of quantum computation using the knowledge about them. Moreover, due to their classical nature, they will naturally help us to analyse quantum computation using classical computers. In order to support the idea, we show two classical methodologies, abstract interpretation and classical public-key cryptography, enhance analysis in two topics of quantum computation, entanglement in quantum programming languages and blind quantum computation protocols.

The behaviour of entangled quantum system is counterintuitive. Therefore, it is important to know how entangled states are in quantum programs without executing them. In order to statistically analyse the problem, it was proposed to apply the abstract interpretation technique to the analysis. However, the proposed method

does not store information about entangled states and ignores the fact that a operator on multiple qubits may undo entanglements, and hence the method only gives a rough approximation. We combine the method with the stabiliser formalism. We show abstract interpretation can be used to efficiently analyse the existence of entanglement in quantum programs with higher precision.

Blind quantum computation protocols give users having no powerful quantum devices a method to delegate their quantum computation to remote quantum servers without leaking any crucial information about their computation. Some protocols enable users to verify whether the quantum servers honestly do the delegated computation, but no protocols give third parties ways to analyse the computation. We propose a new blind quantum computation protocol using a classical public-key encryption scheme. Our protocol is based on an existing protocol, but third parties, who have only classical computers and check the classical message between users and quantum servers, can analyse the computation and verify whether users obtain the correct outcomes or not.

These results show classical methodology, which achieves a development outside the area of quantum computation, may be useful for investigation of quantum computation.