Title	補助ビットを用いた量子回路の並列化手法について
Author(s)	安倍，秀明
Citation	
Issue Date	2000-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/1326
Rights	
Description	Supervisor:平石 邦彦，情報科学研究科，修士

Parallelization of Quantum Circuits using Ancillae

Hideaki Abe

School of Infomation Science,
Japan Advanced Institute of Science and Technology

February 15, 2000

Keywords: quantum circuits, quantum gates, ancillae, depth.

Quantum computer is a new-type computer based on quantum mechanics. As models of quantum computer, D. Deutsch proposed *Quantum Turing machines* and *Quantum circuits*. The former model is proposed as a model of sequential quantum computation, and the later model is proposed as a model of *parallel quantum computation*. It has been proven that the computational power of quantum Turing machines and quantum circuits are polynomially equivalent.

In this thesis, we concerned with quantum circuits. As a model of parallel quantum computation, depth of quantum circuits corresponds to the computing time. It is natural to consider whether we can construct quantum circuits with small depth. The objective of this thesis is to reconstruct quantum circuits for reducing depth, i.e., *to parallelize quantum circuits*, by effectively using available computational resources. Here, the parallelization of quantum circuits is realized by using the computational resources, called *ancillae*. Intuitively, ancillae are additional input bits of quantum circuits in the sense that the outputs of quantum circuits do not depend on the states of ancillae. As results of using ancillae, essentially, it allows us not only to store information in it, but also *to put more quantum gates in parallel*.

We proposed several techniques for parallelizing quantum circuits. Our parallelization techniques are proposed for three types of quantum circuits: 1) quantum

circuits consist of *controlled-not gates*, 2) quantum circuits consist of *controlled-not gates* and *phase-shift gates*, 3) quantum circuits consist of *controlled-not gates* and *Walsh-Hadamard gates.* The controlled-not gates are quantum gates with two inputs, and the Walsh-Hadamard gates are quantum gates with one input. All the phase-shift gates used in the second type are restricted to have the same number of inputs. Nonetheless, the number of inputs of those gates is allow to be fixed arbitrarily.

As previous results, C. Moore and M. Nilsson showed that for any quantum circuit of the first and third type with n inputs, the depth can be reduced to $O(\log n)$ by using $O(n^2)$ ancillae, and for any quantum circuit of the second type with n inputs, the depth can be reduced to $O(\log n + \log s)$ by using $O(lsn + n^2)$ ancillae, if the quantum circuit contains s phase-shift gates and each of which has l inputs.

Our main results are proposing efficient parallelization techniques for the three types of quantum circuits for the case that the number of available ancillae is arbitrarily fixed. As special cases of our results, we have shown that for any quantum circuit of the three types with n inputs, the depth *still* can be reduced as in the previous results, *even if* the numbers of used ancillae are reduced from the previous results by $1/\log n$. Furthermore, our result for quantum circuits of the second type can be extended to the case when the above restriction (i.e., all the phase-shift gates have the same number of inputs) does not exist.

Finally, for the three types of quantum circuits, no technique for proving nontrivial lower bounds of the number of ancillae for parallelizing quantum circuits to have desired depths is known. To find such technique is one of the most interesting open problems of quantum circuits. In our results, we have shown that if the number of available ancillae is arbitrarily fixed, say m, any quantum circuits of the first type with n inputs can be parallelized to have depth at most $O(n^2/(n+m))$. We conjecture that this upper bound is *tight*, i.e., we conjecture that there exists some computation U which can be realized by quantum circuits of the first type, and such that the minimum depth of quantum circuits of the first type which realize U is $\Omega(n^2/(n+m))$.