大規模な量子回路の効率的な設計手法に関する研究（042107003）

Studies on Efficient Design Methods for Large Quantum Circuits

研究代表者

山下　茂　国立大学法人　奈良先端科学技術大学院大学 情報科学研究科

Shigeru Yamashita Graduate School of Information Science, Nara Institute of Science and Technology

研究期間　平成 16 年度～平成 18 年度

本研究開発の概要

次世代の計算機として注目されている量子計算機を具体的に利用するための方法論は、現在まだ確立されていない。そこで、本研究では、世界に先駆けて、高級言語で書かれた量子アルゴリズムから量子計算機デバイス上の基本演算の列（量子回路）を効率よく生成する手法の開発を行なった。この手法は将来の量子計算機の利用には不可欠なため、他国に先駆けて本研究を推進したことは我が国にとって有益であると考えられる。本研究構想では、この目的のために以下の 4 つの要素技術、（1）量子アルゴリズムを記述するための高級言語、（2）量子計算機と古典計算機を協調させて利用する手法、（3）量子アルゴリズムの記述を基本ゲートの回路に変換する手法、（4）（3）で生成される量子回路を対象とする物理系の基本演算に変換する手法の枠組み、などに関して重点的に研究を行った。また、関連研究としてGrover Searchを効率よく利用する計算手法の開発なども行った。

Abstract

It has not been well studied how to utilize quantum computers concretely. Thus, this research aimed to develop the first methodology to transform a quantum algorithm written by a high-level language into a sequence of basic operations (quantum circuit) on quantum computational devices. This methodology is indispensable for the future quantum computation, and thus it should be very important to develop the research. For the purpose, the followings have been studied: (1) high-level language for quantum computation, (2) cooperation between quantum and classical computers, (3) transformation from quantum algorithms into basic quantum gates, and (4) transformation from quantum gates into physically basic operations. As related research topics, how to utilize Grover Search has also been studied.

１．まえがき

現在の計算機（以下では、古典計算機と呼ぶ）の方式では、LSI の微細化が原子のレベルまで進めばその性能が物理的な限界に突き当たると考えられている。また、古典計算機の計算モデルでは、大きな数の因数分解などは、計算時間がかかりすぎるために実質的には計算不能であると考えられている。それに対し、量子力学的な現象をうまく制御して計算を行う計算機（量子計算機）は、原子レベルの量子状態を積極的に利用しようとするもので、上記の因数分解なども現実的な時間で計算可能であることもわかっており、次世代の計算機として近年脚光を浴びている。

技術的に量子計算機の物理的なデバイスはまだ完全に実現されていないが、量子計算機の演算実行はなんらかの物理系の量子状態を実際にコントロールする基本的な演算の列（量子回路）で実現するのが最も妥当だと考えられる。つまり、現在考えられている量子アルゴリズムは実際には量子回路に変換してから実行されるものだと考えられる。また、初期の量子計算機は規模が小さいと思われるため、古典計算機とうまく併用する方法が効率の良い利用の仕方だと考えられる。

そのため、現在提案されている様々な量子アルゴリズムを実際に動かすには、量子計算機の物理デバイスを開発することに加えて、利用方法という観点からは、以下の二つの手法が必須となると考えられる。

(1)量子アルゴリズムを量子回路に変換する手法

(2)量子計算機を古典計算機と協調させて利用する手法

これらは、現在の計算機におけるコンパイラのような働きに対応するが、単純に古典計算向けのコンパイラなどの技術を流用することができないため、現状では実用的な規模の（つまり大規模の）量子回路を設計する手法の開発は容易ではない。また、大規模な量子状態を長い時間所望の状態で制御することは難しいため、現実問題としては、使用できる量子ビット数（回路の入力）および回路の段数はできるだけ小さなもの（つまり、高品質の量子回路）を生成しなければならない。そして、もちろん実用的な規模の問題に対して人手で量子回路を設計することは不可能であるため、自動的に設計する手法は不可欠であると考えられている。また、現時点までに決定的な手法が提案されていないように、量子回路の設計手法の確立は古典計算機向けのものに比べて格段に難しいと考えられる。以上の理由から、大規模な量子回路を自動設計するための要素技術に関して、現時点から地道な研究が必要であると考えられる。

以上の状況を考慮して、本研究では、来るべき量子計算の時代の到来にそなえ「量子アルゴリズム記述から効率的な量子回路を設計するシステム」の構築とそれに関連する要素技術、特に大規模な量子回路の現実的な設計手法に関して様々な新しい手法を考案した。

２．研究内容及び成果

前章で述べたとおり、本研究では、量子計算機と古典計算機を協調利用する枠組みを開発した。特に量子計算機の利用方法としては現在唯一の汎用的な量子アルゴリズムとして知られている「Grover Search」を利用することを念頭にプロトタイプの設計支援システムを作成した。そのシステムの概略図を図 1 に示す。この枠組みは以下のとおりである。

まず、プログラムは通常の C++のプログラム記述の中で for ループの中の if 文で探索を行っている箇所で量子探索に置き換えても論理的に問題ないと思われる箇所の直前にＣ＋＋のコメント文で、//Quantum Search と記述する。それにより開発したプロトタイプシステムでは、以下のことが自動的に行われる。

(1)　システム側はその部分を Grove Search で行うべきかを自動で判定し、エラーも考慮して、繰り返しの分

も含めて量子回路を生成する。また、古典計算機からの呼び出しインターフェースも自動で生成する。加えて量子計算機が失敗する場合も考慮にいれて古典計算機でもスレッドとして同時に探索を行うルーチンも実行するように生成し、実行時には量子計算と古典計算のうち先に解を見つけたほうを採用する仕組みを全て自動合成する。

(2) Grover Search をＣ＋＋でシミュレーションするサブルーチン関数も用意しておき、その関数への引数を自動生成する。（そのため実際の量子計算機を用いなくても、時間はかかるが通常のＣ＋＋の環境でも実行結果を検証可能となる。）

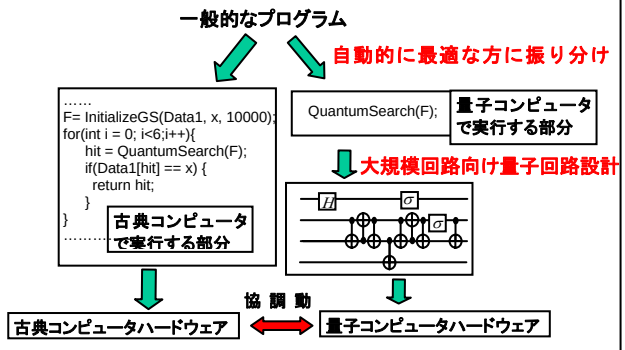

図1　開発した大規模量子回路設計支援システム

量子探索は古典計算機よりも高速に探索が行えると関数の評価回数の観点からは示されている。しかし、量子計算は古典計算に比べて基本演算に対する制約が大きいため、古典計算で行えることを量子計算で実行するにはより多くの基本演算のステップを要する場合も多い。そのため、実際には量子計算で探索を行っても高速化できない場合もあり、そのような場合には、探索を逆に古典計算機で実行させるべきである。本研究で開発した設計環境により、まさにそのような量子計算機と古典計算機の協調利用を有効に利用することが自動で行えるようになった。

上述した枠組みでは、与えられた（大規模な）論理関数を実現する量子回路を設計する手法が必要となる。これに関連して、以下のような研究成果をあげた。

上述した枠組みでは、算術演算を計算する回路が必要となる。それに対して特に 2 つの数を比較する量子回路について、1 ビットに関しては最小であると証明することが出た量子比較回路を考案した。

さらに、量子回路における論理関数のドントケア条件を計算する手法を考案し、実際にプログラムを作成した。これを基にして、いったん合成した量子回路をさらに簡単化するためのプログラムが作成可能となる。

また、大規模な量子回路を組織的に設計する手法として、FDD（Free Decision Diagram）と呼ばれる決定グラフから一般化したトフォリゲートの量子回路を合成する組織的な手法を考案した。

さらに回路設計では重要な「2 つの合成した回路の等価性判定」を効率よく行うために、量子ビットに操作する変換を表現する行列を入力変数の関数と考えて、それを二分決定グラフで表現する Decision Diagram for a Matrix Function (DDMF)というデータ構造を提案した。DDMF によると等価性判定は定数時間で行うことができ、さらにその合成時間や使用するメモリ量も既存の手法に比べ格段に効率がいいことがわかった。

考案した図 1 の枠組みでは、Grover Search を量子計算の利用方法として想定したが、関連研究としてその他の利用方法についても新たな知見を得るために量子計算や量子通信の今までに知られていない利用方法に関して検討を行った結果、種々の新しい学術的な知見を得た。

３．むすび

本研究の成果は、以下の 2 つの用途に用いることができると考えている。

まず一つ目は、実際に量子計算機が物理的に実現した時に、それを使いこなす必須な技術として用いることが期待できる。つまり、将来的に、（古典計算機と協調して動作する）量子計算機システムを利用するための、現在の計算機における OS やコンパイラといったものに相当する部分の中核となる技術として使えると考えられる。 逆にいうと、本技術がなければ将来の量子計算を利用することは難しいと考えられる。そのため、量子計算が実現したときには、本技術は我が国の当該分野の競争力の向上に寄与すると考えられる。

また、量子計算機が物理的に実現する以前にも、以下のような学術的な用途が考えられる。それは、量子アルゴリズムの設計および評価のためのツールとして利用することである。例えば、Grover Search を使って問題を解くときに実際に古典計算機と比べてどのくらい高速になるかを具体的なアプリケーションにおいて見積もることが本研究開発で作成した量子回路設計システムを用いれば可能となり、量子計算がどのような状況でどのように利用できるかを検証することがより容易になる。

以上より、本研究の成果は将来の量子計算システムの実現に向けて不可欠なものであると考えられ、欧米など主要な国でその技術の権利化を行った意義は大きいと考えられる。また、本研究では最終目標にいたるまでに、関連する研究なども多角的に行い、様々な要素技術の確立を行った。そのため、学術的な貢献として、量子回路設計の分野に今まで考えられていなかったような新しい研究テーマを数多く生み出した。今後はそのような成果を基に多くの関連研究が推進されることが期待できる。

【誌上発表リスト】

[1] S. Yamashita, “A Design Method for Large-scaled Quantum Circuits”, COE workshop for SoC Design Technology and Automation P-1-7(2005 年 9 月 15 日)

[2]S. Yamashita, “How to Utilize Grover Search in General Programming”, Laser physics, Vol. 16, No. 4 pp.1-5（2006 年 3 月）

[3]S. Yamashita, D. Michael Miller, “Decision Diagram Data Structure to Represent Quantum Circuit”, 電子情報通信学会技術研究報告 VLD2006-58 pp. 41-46（2006 年 11 月 28 日）

【申請特許リスト】

[1]山下茂、量子コンピュータを含むコンピュータシステムのためのプログラム開発支援装置、プログラム開発支援用プログラム、およびシミュレーション装置、日本、2004 年 12 月 9 日

[2]山下茂、量子コンピュータを含むコンピュータシステムのためのプログラム開発支援装置、プログラム開発支援用プログラム、およびシミュレーション装置、PCT 全指定国際特許、2005 年 8 月 22 日

[3]村上ユミコ、中西正樹、 山下茂、量子暗号通信方法、PCT 全指定国際特許、2007 年 2 月 15 日

【本研究開発課題を掲載したホームページ】

http://qc.naist.jp/SCOPE