

氏名	モハンマド ベライエット アリ Md Belayet Ali
本籍 (国籍)	バングラデシュ
学位の種類	博士 (工学)
学位記番号	工博 第293号
学位授与年月日	平成31年3月22日
学位授与の要件	学位規則第5条第1項該当 課程博士
研究科及び専攻	工学研究科電気電子・情報システム工学専攻
学位論文 題目	Logic Synthesis and Optimization of Reversible and Quantum Circuits for Arithmetic Logic Units (算術演算装置の可逆及び量子回路の論理設計と最適化)
学位審査委員	主査 教授 永田 仁史 副査 教授 萩原 義裕 副査 講師 平山 貴司 副査 准教授 山中 克久

論文内容の要旨

In this thesis, we focus on the logic synthesis and optimization of reversible and quantum circuits for arithmetic logic units (ALUs). The main concept of our approach differs from those of existing related studies, in that we emphasize the function design. Our approach to investigating reversible functions includes (a) embedding of irreversible functions into incompletely-specified reversible functions, (b) operation assignment, and (c) permutation of function outputs. We provide some extensions of these techniques for further improvement in the design of reversible functions. Furthermore, we propose a minimization algorithm to obtain the minimum multiple-control Toffoli (MCT) circuits and a greedy algorithm to reduce the quantum circuits. The organization of our thesis is as follows.

Chapter 1 focuses on the motivation, objectives, and contributions of our study. Reversible computing is generally considered to be an unconventional form of computing, which has drawn considerable attention from researchers in order to design low power computing devices. The ALU is a key element for any programmable computing devices. In the design of an ALU, the adder/subtractor block is a key element. A faster adder/subtractor block will increase the efficiency of the ALU performance as well as that of the entire system. The objective of this thesis is to design ALUs and adder/subtractor blocks that achieve a higher performance and lower power consumption than those of existing systems.

Chapter 2 describes some preliminaries of reversible and quantum logic. Reversible logic has the same number of inputs and outputs and has a one-to-one mapping between the vectors of the inputs and outputs. Thus, the vector of the input states can always be reconstructed from the vector of the output states. The most promising application of

reversible logic is quantum computation. Researchers have utilized quantum computation to solve many relevant problems faster than by traditional computing machines. For example, the factorization problem can be solved in polynomial time using quantum computation, whereas, only exponential algorithms are known for traditional machines.

Chapter 3 describes related work, and problems in previous synthesis and optimization approaches. In recent decades, the Toffoli, Peres, and Fredkin gates have conventionally been used to synthesize reversible circuits, and we adopt the MCT gate library to design a reversible adder/subtractor and simple ALU circuits. Several ALU and adder/subtractor designs were investigated based on reversible logic. We found that related approaches for reversible adder/subtractors and ALUs lacked analysis on the level of the reversible functional design. In this thesis, we focus on the logic synthesis and optimization of reversible and quantum circuits for arithmetic logic units by emphasizing the functional design.

Chapter 4 describes the unique and interesting aspect of our idea for the improvement of reversible circuits. The overall process for reversible circuit synthesis is different from those in related approaches. We attempt to achieve improvements on the level of the function design. Our approach to investigating the reversible functions includes the following:

- The embedding of irreversible functions into incompletely-specified reversible functions. To obtain a reversible circuit of an irreversible function, we first embed the irreversible function into an incompletely-specified function to make it reversible. In this work, we set a restriction in which only minimum necessary ancilla lines (additional input Boolean variables for constructing the output function) are added for embedding.
- The operation assignment is the unique and interesting aspect of our idea for improving reversible circuits. This is a permutation of groups of rows in the truth table. Even if the set of operations is the same, the functions consisting of those operations vary according to the assignment of the operations. Our approach is to try all permutations of operations and find the minimum circuit realization.
- We have employed the idea of permuting the outputs of a reversible function called synthesis with output permutation (SWOP), as introduced in the book by Wille et al. SWOP can easily be applied by encoding all output permutations, synthesizing each in one turn, and keeping the best one.

Chapter 5 describes the proposed minimization algorithm for obtaining the minimum MCT circuits. Our minimization algorithm consists of a combination of the equivalence classes of the operation assignment and permutation of function outputs, and the minimization problem is extended to a further reduction of gates in a circuit. We use the hash tables of minimum MCT circuits with up to seven gates for 4-bit functions and five gates for 5-bit functions. The tables are simply constructed using an exhaustive enumeration of gate combinations.

Chapter 6 describes the reduction of the quantum circuits. We obtain quantum circuits for our reversible adder/subtractors and ALUs by applying a greedy algorithm. This

algorithm performs the transformation of a given MCT circuit into a quantum circuit, searches a pair of adjacent gates in the circuit by moving the gate according to the moving rule, and applies various reduction rules to obtain the reduced quantum circuit. The execution of moving and reducing the gates is repeated if the quantum gates in the quantum circuit are successively reduced. The experimental results show that our proposed designs are superior to existing designs in terms of the numbers of input lines, constant inputs, garbage outputs, and the quantum cost.

Finally, Chapter 7 describes our conclusions and future works. In this thesis, we present the minimum MCT circuits that realize adder/subtractors and some benchmark ALUs. To improve the function design, our idea involves the unique and interesting aspect of a minimization algorithm to obtain the minimum MCT circuits, and a greedy algorithm to obtain the reduced quantum circuits. Although research in this area is still in the early stages, the existence of promising application in future computing devices motivates further research in this direction. Recently, the linear nearest neighbor (LNN) architecture has received intense attention from a practical view point, and with respect to various nanotechnologies, where each qubit can interact with at most one neighbor above and one neighbor below. According to the different technological constraints, we are considering to revise our synthesis approach and design more practical reversible and quantum adder/subtractors and ALUs. Furthermore, it should be investigated whether our proposed functional design approach can be adopted for additional arithmetic/logic operations and other universal gate sets.

論文審査結果の要旨

加算、減算などの算術演算や AND、OR などの論理演算を担う演算装置 (ALU: Arithmetic Logic Unit) は、計算機の最も重要な構成要素の一つであり、ALU の高性能化は、計算機を用いたシステム全体の性能向上をもたらす。近年、可逆論理に基づいた ALU の構成法が研究されている。可逆とは、多出力論理関数が全単射であることを意味する。可逆論理は、情報の損失がないことから、高性能計算や低消費電力化に向いており、量子ゲート方式の量子コンピュータを実現するための基礎理論としても注目されている。

本論文は、可逆加減算器や可逆 ALU の最適合成を提案している。ここで、最適化の目標は、回路のゲート数の最小化である。可逆論理合成は、通常デジタル回路の合成とは大きく異なる技術である。可逆論理合成の手順は、上流から順に、可逆論理関数の設計、可逆回路合成、量子回路合成の 3 段階から成る。関連研究は、可逆回路合成から下流の段階の議論が主であるが、提案手法は、上流段階の可逆論理関数の設計を工夫することにより、下流段階で合成される回路のゲートを効果的に削減する点が独創的である。可逆 ALU の論理が持つ対称性に着目して可逆論理関数の同値類を提案し、ALU の最適化問題を ALU の同値類の最適化問題に一般化している。この理論を応用することにより、従来より少ないゲートで可逆回路や量子回路が合成できることを実験により実証している。

以下に論文の具体的な内容を示す。

第 1 章は導入であり、可逆論理合成の研究背景を述べている。特に、ALU を可逆論理で実現することの意義と有用性を説明している。

第2章は、可逆論理関数、可逆回路、量子回路、これらの回路で使用されるゲートなど、基本的な構成要素の定義を行っている。可逆回路で使用されるゲートは、NOT、CNOT、Toffoli とし、量子回路で使用されるゲートは、NOT、CNOT、制御 V、制御 V⁺ としている。これらは可逆論理合成における最も標準的な仮定であり、広く使われている。

第3章は、関連研究に関する文献調査である。これまでの可逆 ALU の研究は、可逆回路合成もしくは量子回路合成の段階の最適化であり、上流段階の可逆論理関数の設計の観点が欠落していることを本章で指摘している。

第4章は、可逆論理関数の設計の工夫であり、これが可逆加減算器や可逆 ALU の最適合成を進歩させた本研究の中心的な理論である。具体的には、(1) 不可逆である ALU の論理を可逆論理関数に埋め込む手法、(2) ALU で用いられる演算の割り当て順序に着目した可逆論理関数の演算割当同値類、(3) ALU の出力線の並び順に着目した可逆論理関数の出力置換同値類、の3点である。提案する同値類は、ALU として等価な機能を持つ可逆論理関数の集合である。そのため、ALU としては、同値類のどの可逆論理関数を合成してもよい。一方、提案する同値類においては、可逆論理関数としては同値でも、合成される回路のゲート数は一般に異なる。この議論より、同値類の中からもなるべく少ないゲートで合成される回路を選択する、という最適化戦略が取れるようになった。この戦略に基づき、ALU の最適化問題を ALU の同値類の最適化問題に一般化し、提案する同値類を回路合成に応用するための理論構築をしている。提案手法は、ALU の論理的特性を可逆論理関数の設計に巧みに応用するものであり、画期的である。この後の第5章と第6章で、提案手法を用いた回路合成の実験を行っている。

第5章は、ALU の可逆回路合成である。ゲートの網羅的な組み合わせを探索する方法による可逆回路合成アルゴリズムを用いて、ALU の最適化を実験している。演算割当同値と出力置換同値を併用した同値類を最小化することにより、半加減算器、全加減算器、各種ベンチマーク ALU について、従来よりもゲートの少ない可逆回路が得られている。ゲート数が83%削減された ALU もあり、提案手法の有効性が実証されている。

第6章は、ALU の量子回路合成である。第5章で得られた可逆回路を量子回路に変換し、貪欲法による単純化アルゴリズムを用いて、量子回路を合成している。従来の量子回路と比較して、ゲート数が最大で87%削減されるなど、量子回路合成においても有効であることが示されている。

第7章は、結論であり、今後の課題や応用についても述べている。

以上のように、本論文は、可逆論理合成における可逆論理関数の設計に着目し、加減算器や ALU の論理的特性を活用した可逆論理関数の同値類（演算割当同値、出力置換同値）を提案し、ALU の最適化問題を ALU の同値類の最適化問題に一般化した。回路合成の実験を通して、可逆回路や量子回路のゲートを効果的に削減することに成功しており、提案手法の有効性が確認された。これらの成果は、可逆論理合成の研究の発展に大いに寄与するものである。

よって、本論文は博士（工学）の学位論文として合格と認める。

原著論文名（1編を記載）

M. B. Ali, T. Hirayama, K. Yamanaka, and Y. Nishitani. Function design for minimum multiple-control Toffoli circuits of reversible adder/subtractor blocks and arithmetic logic units. *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E101-A, No. 12, pp. 2231–2243, December 2018.