様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ３０ 日現在

機関番号：１１２０１
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５０００５３

研究課題名（和文）可逆論理回路合成のための新しい論理式のクラスとその最小化アルゴリズム

研究課題名（英文）A new class of expressions for reversible logic synthesis and its minimization algorithm

研究代表者

平山　貴司（HIRAYAMA, Takashi）

岩手大学・工学部・講師

研究者番号：３０３１６５０９

交付決定額（研究期間全体）：（直接経費）　　1,600,000円

研究成果の概要（和文）：量子コンピュータの実現には、なるべく量子論理ゲート数が少ない可逆論理回路を論理合成することが望ましい。本研究の特色は、可逆論理回路の最小化を行うために、AND-EXOR論理式の新しいクラスAESPを提案したことである。これにより、可逆論理回路のゲート数最小化問題は、AESPの積項数最小化に帰着できるようになった。加えて、AESPの最小化アルゴリズムや可逆論理回路のゲート数の下界を提案した。本研究の成果は、量子回路の実現と、将来の量子コンピュータの実現のための基礎として貢献する。

研究成果の概要（英文）：The reversible logic synthesis with as fewer quantum gates as possible is required to implement quantum computers. The novelty of this research is that a new class of AND-EXOR expressions, AESPs, is proposed in order to synthesize reversible circuits. Consequently, the minimization problem of gates in reversible circuits has been reduced to the minimization of products in AESPs. Moreover, minimization algorithms for AESPs and lower bounds on the gate count of reversible circuits have been presented. These results contributes to the synthesis of quantum circuits and possibly to the implementation of future quantum computers.

研究分野：情報工学

キーワード：可逆論理回路　AND-EXOR論理式

１．研究開始当初の背景

量子コンピュータは、理論上任意の並列度で計算を行うことが可能なコンピュータであり、現在のディジタルコンピュータの延長とは本質的に異なる高い計算能力を持つ。しかしながら、量子コンピュータは、現在、基礎研究の段階であり、実現されていない。量子コンピュータの世界初の実現に向けて、国内国外を問わず、多数の研究機関が量子回路の研究でしのぎを削っている。量子回路の論理合成レベルの基本モデルは可逆論理回路であり、NOT ゲート，CNOT ゲート，Toffoli ゲートなどの量子論理ゲートを組み合わせて構成される。効率の良い量子回路を実現するためには、なるべく量子論理ゲートの段数が少ない可逆論理回路を論理合成することが望ましい。

２．研究の目的

国内の研究者によって、「論理関数の積項数最小の AND-EXOR 論理式を求めることが、段数最小の f-C-NOT 型量子回路を論理合成することに対応する。」という定理が近年発表された。

AND-EXOR 論理式は、ディジタル回路の基本モデルの一つであり、AND-EXOR 論理式の積項数最小化は、元々は排他的論理和(EXOR)演算を活用したディジタル回路設計の基礎理論として研究されてきた。申請者は、これまで AND-EXOR 論理式を研究してきており、高速な AND-EXOR 論理式最小化アルゴリズムを開発したことにより、実用的な論理関数について、世界で初めて厳密な最小形を計算することに成功し、その研究成果を発表した。この結果と上記の定理を合わせることにより、f-C-NOT 型量子回路の厳密な最小形が明らかになった。

しかし、上記の定理は f-C-NOT 型量子回路に限定した性質であるため、他の可逆論理回路にはそのままでは適用できない。一般的な可逆論理回路を合成するには、それに適した新しい論理式のクラスとその最小化アルゴリズムが必要である。f-C-NOT 型量子回路も一般的な可逆論理回路も、NOT ゲート，CNOT ゲート，Toffoli ゲートなどの量子論理ゲートを組み合わせて構成される。これらのゲートの論理動作は AND 演算と EXOR 演算である。そのため、f-C-NOT 型量子回路も可逆論理回路も、AND と EXOR の論理で表現される点は同じである。違いは、量子論理ゲートの並び順に関する制約である。f-C-NOT 型量子回路では、回路が実現する論理関数は量子論理ゲートの並び順に依存しないため、量子論理ゲートを積項に対応させることで、AND-EXOR 論理式で表現することができた。AND-EXOR 論理式では、積項の並び順は論理式が実現する論理関数に依存しない。一方、可逆論理回路では、回路が実現する論理関数は量子論理ゲートの並び順に依存する。このため、可逆論理回路の合成には、AND-EXOR 論理式の積項に、論理ゲートの並び順を反映する制約を付けた新しい論理式のクラスを考えなければならない。

本研究の特色は、可逆論理回路の最小化を行うために、申請者の AND-EXOR 論理式の技術を応用しようとする点である。本研究では、可逆論理回路に対応した AND-EXOR 論理式のクラスを明らかにし、その最小化アルゴリズムを開発することを目指す。最小化アルゴリズムが開発されることにより、実用的な論理関数について段数の少ない可逆論理回路を効率良く論理合成することができるようになる。

３．研究の方法

本研究の目標は、可逆論理回路を表現する AND-EXOR 論理式の新しいクラスを提案し、その論理式の最小化アルゴリズムを開発することである。そのために、従来の AND-EXOR 論理式および最小化アルゴリズムと、可逆論理回路の性質とを比較し、論理ゲートの並び順を反映する制約など論理式が持つべき適切な条件を見出し、新しい論理式のクラスの提案とアルゴリズムの改良を行った。

まず、可逆論理回路のモデルと性質について情報収集を行い、AND-EXOR 論理式と可逆論理回路との対応について検討した。AND-EXOR 論理式に基づいた可逆論理回路設計としては、従来は PPRM(正極性 Reed-Muller 論理式）や FPRM（固定極性 Reed-Muller 論理式）が用いられてきた。これらの論理式から得られる可逆論理回路では、論理ゲートの並び順は任意であり、論理ゲートの並び順は回路が実現する論理関数に影響しない。しかし、このような可逆論理回路は特殊な部類であり、本来の可逆論理回路は論理ゲートの並び順に依存する多段回路である。そのため可逆論理合成においては、論理ゲートの並び順を考慮する方がより段数の少ない可逆論理回路になる。原理的には、AND-EXOR 論理式の積項は論理ゲートに対応するが、より段数の少ない可逆論理回路を合成するためには、論理ゲートの並び順を論理式に反映するような制約を考慮しなければならないことがわかった。

そこで、本研究では、リテラルの極性の出現順序に適切な制約を加えた新しい論理式のクラスを提案し、AESP(AND-EXOR expression with Shifting Polarities)と名づけた。AESP は以下の条件 1，2 により再帰的に定義される AND-EXOR 論理式である。

条件1.　定数論理式 0，1 は AESP である。

条件2.　X_{n-1} を変数集合$\{x_1, x_2, \cdots, x_{n-1}\}$とし、$G_1$を$X_{n-1}$を持つ PPRM、$G_0$，$G_2$を$X_{n-1}$を持つ AESP とすると、$x_n G_1 \oplus \bar{x}_n G_0 \oplus G_2$ はn変数 AESP である。

AESP の定義より、「各積項において、変数x_iのリテラルが肯定リテラルならば、$j < i$となる変数x_jのリテラルは肯定リテラルである。また、各積項において、変数x_jのリテラルが否定リテラルならば、$j < i$となる変数x_iのリ

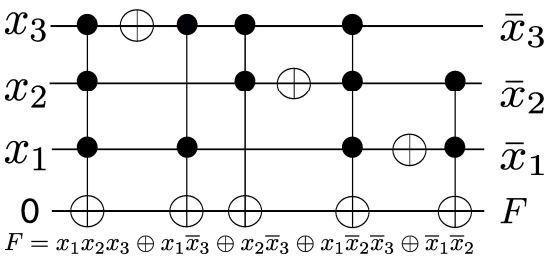

図 2：AESP の例 1

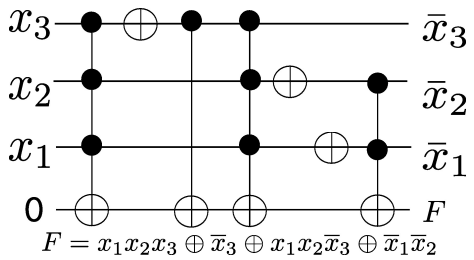

図 1：AESP の例 2

テラルは否定リテラルである。」という性質が得られる。この制約は、PPRM や FPRM におけるリテラルの極性の制約よりも自由度があり、その結果、AESP は、PPRM や FPRM よりも少ない積項で論理関数を表現できる。これは従来よりも少ない論理ゲートで可逆論理回路を合成できることを意味する。AESP の積項における否定極性の現れ方に対応して NOT ゲートを配置することにより、AESP の積項から可逆論理回路の論理ゲートの並び順が定まるようになった（図 2、図 1）。このように AESP から可逆論理回路へ変換するアルゴリズムを与えた。この結果、可逆論理回路の最小化問題は AESP の最小化に帰着できるようになった。

次に、AESP の最小化アルゴリズムの開発を行った。AESP は再帰的に定義される AND-EXOR 論理式である点に着目し、論理関数のすべての部分関数について再帰的に最小化することで、解の最小性を保証できるアルゴリズムを開発した（図 3）。ここで、規模の小さい関数、具体的にはm変数以下の関数については、最小 AESP が予め表に格納されているものとしている。この最小化アルゴリズムは、計算時間がかかることが欠点である。理論的には、与えられる論理関数の変数の個数をnとすると、最小化アルゴリズムの時間計算量は、$O(n2^{n+2^n})$である。計算機実験をしたところ、実用上は最小化できるのは 5 変数関数までであることが確認された。

規模の大きな論理関数にも対応できるようにするため、最小性の保証を犠牲にする代わりに、最小に近い解を高速に求める簡単化アルゴリズムの開発を行った。計算時間のかかる原因は、調べる部分関数の個数が$2^{2^{n-1}}$個と多いためである。さまざまな部分関数の集合について計算機実験を重ねた結果、シャノン展開に関するわずか 8 個の部分関数について調べれば、多くの場合最小に近い解が求められることがわかった。そこで最小化アルゴリズムを、8 個の部分関数について再帰的に

```
1: function aesp(f)
2:     if n ≤ m then
3:         return (f の最小 AESP)
4:     end if
5:     F_min := (a large dummy)
6:     for g in F^{n-1} do
7:         F_1 := pprm(f_{x_n=1} ⊕ g)
8:         F_0 := aesp(f_{x_n=0} ⊕ g)
9:         F_2 := aesp(g)
10:        F := x_n F_1 ⊕ x̄_n F_0 ⊕ F_2
11:        if τ(F) < τ(F_min) then
12:            F_min := F
13:        end if
14:    end for
15:    return (F_min)
16: end function
```

図 3：AESP の最小化アルゴリズム

計算するように変更することで、高速な簡単化アルゴリズムを得た。計算機実験により、10 変数関数の簡単化が可能であることを確認した。

また、可逆論理回路の論理ゲートと AND-EXOR 論理式の積項の対応について研究する中で、可逆論理回路を合成する際に必要なゲート数の下界を求める手法を開発した。定理：任意の可逆論理関数Fについて、$\gamma(F) \geq \sigma\text{-}lb(\Lambda(F))$が成り立つ。

ここで、$\gamma(F)$はFの最小な可逆論理回路のゲート数である。可逆論理関数Fのすべての出力について論理式の積項数を求め、整数のベクトル$\Lambda(F)$を作る。そのベクトル演算に基づいた下界$\sigma\text{-}lb(\Lambda(F))$を提案し、それが従来の下界よりも良いことを理論的に証明した。加えて、その高速な計算方法を与えた（図 4）。さらに、逆関数やゲートの性質を利用することで、下界を改良した。ベンチマーク関数に対する計算機実験により、多くの論理関数について、従来より良い下界が明らかになった。

以上の研究におけるアルゴリズムの開発や計算機実験には、本研究費で購入した PC を使用した。

4．研究成果

主な研究成果のまとめは下記の通りである。

(1) AND-EXOR 論理式の新しいクラス AESP(AND-EXOR expression with Shifting Polarities)を提案した。これは、リテラルの極性の出現順序に適切な制約を加えた論理式のクラスである。これにより、可逆論理回路のゲート数最小化問題は、AESP の積項数最小化に帰着できるようになった。

(2) APSP の最小化アルゴリズムを開発した。

```
1: function SigmaLB3(S): Integer          ▷ Input: S is a vector of non-negative integers.
2:     Var min: Integer;
3:     Var ht: Hash Table;
4:     procedure HELPER(S, c)    ▷ Input: S is a vector and c is an integer.
                                          ▷ Side Effect: Updating min.
5:         if c + ⌈log(∑S + 1)⌉ ≥ min then return ;
6:         end if
7:         if S = 0 then
8:             min ← c;
9:             return ;
10:        end if
11:        if ht[rep(S)] = ∅ or c < ht[rep(S)] then
12:            if (all elements of S are even) then
13:                HELPER(Φ(S, 1), c + 1);
14:            else
15:                for i ← 1 to n do
16:                    if (S[i] is odd) then
17:                        HELPER(Φ(S, i), c + 1);
18:                    end if
19:                end for
20:            end if
21:            ht[rep(S)] ← c;
22:        end if
23:    end procedure
24:    min ← a large integer;
25:    HELPER(S, 0);
26:    return min;
27: end function
```

図 4：高速に下界を計算するアルゴリズム

これにより、論理関数から最小な AESP を求めることができるようになった。厳密な最小化アルゴリズムは、解の最小性を保証するが、最小化できるのは規模の小さい論理関数に限られる。

(3) 最小に近い AESP を高速に求める簡単化アルゴリズムを開発した。これは、規模の大きな論理関数について、最小に近い可逆論理回路を実用時間で求めることができる。

(4) 可逆論理回路のゲート数の下界を求める手法を開発した。これにより、従来よりも正確に可逆論理回路のゲート数の見積もりができるようになった。

本研究の結果は、量子回路の実現に貢献する。

量子回路の実現は将来の話であるため、本研究で開発されたアルゴリズムにより、直ちに量子回路の設計が開始されるわけではない。しかしながら、実用関数について最小段数の量子回路を求めるアルゴリズムは、今後の量子回路実現の研究分野において必要不可欠である。本研究の成果は、量子回路の実現と、将来の量子コンピュータの実現のための基礎として貢献する。

５．主な発表論文等

〔雑誌論文〕（計１件）

① T. Hirayama, H. Sugawara, K. Yamanaka, and Y. Nishitani, A lower bound on the gate count of Toffoli-based reversible logic Circuits, IEICE Trans. Information and Systems, Vol. E97-D, No. 9, pp. 2253-2261, September 2014. 査読あり
DOI: 10.1587/transinf.2013LOP0013

〔学会発表〕（計１６件）

① 菅原隼人，平山貴司，山中克久，西谷泰昭．可逆論理回路における Toffoli ゲート数の下界の改良．平成 26 年度第 2 回情報処理学会東北支部研究会，2014 年 12 月 21 日，発表場所：岩手大学工学部（岩手県・盛岡市）

② 松尾亘，山中克久，平山貴司，西谷泰昭．可逆論理回路合成のための AND-EXOR 論理式の簡単化アルゴリズム．平成 26 年度第 2 回情報処理学会東北支部研究会，2014 年 12 月 21 日，発表場所：岩手大学工学部（岩手県・盛岡市）

③ 菅原隼人，平山貴司，山中克久，西谷泰昭．可逆論理回路における Toffoli ゲート数の下界の改良に関する一考察．第 37 回多値論理フォーラム，2014 年 9 月 13 日～2014 年 9 月 14 日，発表場所：関西大学千里山キャンパス（大阪府・吹田市）

④ 平山貴司，西谷泰昭．可逆論理回路における Toffoli ゲート数の下界とその評価．第 27 回多値論理とその応用研究会技術報告，2014 年 1 月 11 日～2014 年 1 月 12 日，発表場所：鹿児島県文化センター（鹿児島県・鹿児島市）

⑤ M. B. Ali and T. Hirayama. Report on reversible logic synthesis and optimization techniques. 平成 25 年度第 4 回情報処理学会東北支部研究会，2013 年 12 月 21 日，発表場所：岩手大学工学部（岩手県・盛岡市）

⑥ T. Hirayama, T. Murayama, K. Yamanaka, and Y. Nishitani. A lower bound on the gate count of Toffoli-based reversible logic circuits. Reed-Muller Workshop 2013, 2013 年 5 月 24 日～2013 年 5 月 25 日，発表場所：富山国際会議場（富山県・富山市）

⑦ 村山達郎，平山貴司，山中克久，西谷泰昭．可逆論理回路における Toffoli ゲート数の下界とその評価．平成 24 年度第 3 回情報処理学会東北支部研究会，2012 年 12 月 22 日，発表場所：岩手大学工学部（岩手県・盛岡市）

６．研究組織

(1)研究代表者

平山　貴司（HIRAYAMA, Takashi）
岩手大学・工学部・講師
研究者番号：30316509

(2)研究分担者

なし

(3)連携研究者

なし

(4)研究協力者

村山　達郎（MURAYAMA, Tatsuro）
ALI, Md Belayet

菅原 隼人（SUGAWARA, Hayato）
松尾 亘（MATSUO Wataru）