A-013

1-CNOT 回路内の縮退故障を検出する検査入力集合生成アルゴリズム

加藤貴昭, 山田敏規
埼玉大学 大学院理工学研究科 数理電子情報部門

1 はじめに

Bennett[1]，Fredkin と Toffoli[2] は可逆回路が任意の小さいエネルギーの消費で機能することを証明した．さらに，可逆回路はデジタル信号処理等の応用が考えられる．したがって、可逆回路は非常に魅力的であると言える．

可逆回路の製造時に回路内の故障を見つけることは重要であるが，可逆回路内の縮退故障，すなわち，一部の配線の値を 0 か 1 に固定する故障を検出する検査入力集合を生成するアルゴリズムはあまり知られていない．Patel ら [3] は，任意の可逆回路 C に対して $|T| = O(\log |W(C)|)$ であるような完全な，すなわち，あらゆる縮退故障を検出する検査入力集合 T が存在することを証明した．$W(C)$ は回路 C に対する配線の集合である．Tabei ら [4] は任意の可逆回路に対して $|T| = O(\log |W(C)|)$ であるような完全な検査入力集合 T を期待多項式時間で生成するような乱択アルゴリズムを提案した．本研究では，0-CNOT，1-CNOT ゲートで構成された任意の回路に対して $|T| = O(n(n+g))$ である完全な検査入力集合を生成する決定性多項式時間アルゴリズムを提案する．

2 可逆回路と完全な検査入力集合

論理ゲートは入力から出力が全単射であるとき，つまり全ての異なる入力に対して，一対一対応する出力が存在するとき可逆である．ある可逆ゲートが k 個の入力ビットと出力ビットを持つとき $k \times k$ 可逆ゲートと呼ぶ．

n を正の整数であるとする．n-入力可逆回路は以下のように再帰的に定義される．

(1) n 本の配線からなる回路は可逆回路である．このとき，配線の一方の端を入力，もう一方を出力と呼ぶ．

(2) C' を n-入力可逆回路とし，G を $k \times k$ 可逆ゲートとする．このとき，C' の出力側の配線の k 本と G の入力を接続することによって得られる回路 C は，n-入力可逆回路である，C の入力は C' の入力であり，C の出力は C' の残りの出力と G の出力である．

(3) n-入力可逆回路は (1) と (2) によってのみ構成される．

ある正の整数 n に対して n 入力可逆回路である回路を可逆回路と呼ぶ．

C を n 入力可逆回路とする．任意の $T \subseteq \{0,1\}^n$ を C に対する検査入力集合と呼ぶ．各入力 $\boldsymbol{x} \in T$ に対する C の出力のみによって C のあらゆる縮退故障が検出できるとき，T は完全であると言われる．

C に含まれる配線 w は，ある $\boldsymbol{x}, \boldsymbol{x'} \in T$ に対して $w(\boldsymbol{x}) = 0$ かつ $w(\boldsymbol{x'}) = 1$ であるとき，T によって制御可能であるという．ここで，$w(\boldsymbol{x})$ は C に対して入力 $\boldsymbol{x}$ があたえられたときの配線 w の値を表す．C の全ての配線が T によって制御可能であるとき，C は T によって制御可能であるという．以下の定理は [3] で証明されている：

定理 1 C が T によって制御可能であるときかつそのときに限り，T は C に対して完全である．

可逆ゲートの一つに CNOT ゲートがある．任意の非負の整数 k に対して，k-CNOT ゲートは $(x_1, x_2, \ldots, x_k, t) \in \{0,1\}^{n+1}$ が入力として与えられたときに $(x_1, x_2, \ldots, x_k, t \oplus (1 \cdot x_1 x_2 \cdots x_k))$ を出力するような $(k+1) \times (k+1)$ 可逆ゲートである．ここで $\oplus$ は排他的論理和を表す．$x_1, x_2, \ldots, x_k$ はゲートの制御ビットと呼ばれ，t は標的ビットと呼ばれる．CNOT 回路は CNOT ゲートのみで構成される可逆回路である．$k' \leq k$ であるような k'-CNOT ゲートのみで構成されている CNOT 回路を k-CNOT 回路という．

3 1-CNOT 回路内の配線の値の計算

C の入力を $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ とすると，次のことが示される．

定理 2 C が 1-*CNOT* 回路であるならば，C の各配線 w の値 $w(\boldsymbol{x})$ を線型関数で表現することができる．

証明: まず，入力の第 i ビット目の配線の値は x_i で表すことができる．

i 番目のゲートの前まで全ての配線の値が線型関数で表現可能であると仮定し，i 番目のゲートの出力について考える．i 番目のゲートが 0-CNOT ゲートであるならば，入力を $a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$ としたとき，出力は $(1 \oplus a_0) \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$ となり，線型関数で表現することができる．i 番目のゲートが 1-CNOT ゲートであるならば，制御ビットの入力を $a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$ とし，標的ビットの入力は $b_0 \oplus b_1 x_1 \oplus b_2 x_2 \oplus \cdots \oplus b_n x_n$ とする．このとき，ゲートの制御ビットの出力の値は入力の値と同一であり，線型関数である．標的ビットの出力の値は $(a_0 \oplus b_0) \oplus (a_1 \oplus b_1) x_1 \oplus, \ldots, \oplus (a_n \oplus b_n) x_n$ と

なり，$(a_0 \oplus b_0), (a_1 \oplus b_1), \cdots, (a_n \oplus b_n)$ は定数であるので，線型関数で表現することができる． ■

定理 2 より $w(\boldsymbol{x})$ は係数ベクトル $\boldsymbol{a} = (a_0, \ldots, a_n) \in \{0,1\}^{n+1}$ で表現することができる．ゲートの数を g とすると，配線の総数は $n + g$ となる．

定理 3 全ての配線 w の値 $w(\boldsymbol{x})$ は $O(n(n+g))$ 時間で計算可能である．

4 提案アルゴリズム

定理 1 と 2 より以下は自明である．

定理 4 $T \subseteq \{0,1\}^n$ が n 入力 1-*CNOT* 回路 C に対して完全であるための必要十分条件は，各配線 W に対する $W(\boldsymbol{x})$ の係数ベクトル $\boldsymbol{a} = (a_1, \ldots, a_n) \in \{0,1\}^{n+1}$ に対して，

$(a_1, a_2, \ldots, a_n) \cdot \boldsymbol{x}^{\boldsymbol{T}} = 0$ である入力 $\boldsymbol{x} \in T$ と

$(a_1, a_2, \ldots, a_n) \cdot \boldsymbol{x'}^{\boldsymbol{T}} = 1$ である入力 $\boldsymbol{x'} \in T$

が存在することである．

次の 2 つの補題も自明である．

補題 1 $\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ と $\boldsymbol{x} = (x_1, x_2, \ldots, x_i) \in \{0,1\}^i (1 \leq i < n)$ が与えられているとする．このとき，$a_j = 1$ である $j (i < j \leq n)$ が存在するならば，$\boldsymbol{a} \cdot \boldsymbol{x} = 0$ となる $\boldsymbol{x} = (x_1, x_2, \ldots, x_i, x_{i+1}, \ldots, x_n)$ と $\boldsymbol{a} \cdot \boldsymbol{x'} = 1$ となる $\boldsymbol{x'} = (x'_1, x'_2, \ldots, x'_i, x'_{i+1}, \ldots, x'_n)$ が存在する．

補題 2 $\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ と $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ が与えられているとする．このとき，$a_j = 1$ である $j (i < j \leq n)$ が存在しない，すなわち $\boldsymbol{a} = (a_1, a_2, \ldots, a_i, 0, \ldots, 0)$ であるならば $(a_1, a_2, \ldots, a_i)$ と $(x_1, x_2, \ldots, x_i)$ の内積の値は $\boldsymbol{a} \cdot \boldsymbol{x}$ と等しくなる．

以上の性質や補題 1，2 を用いてアルゴリズムを構築する．

アルゴリズム TESTSET(C)

Step 1: 検査入力集合 T に $(0, 0, \ldots, 0)$ を加える．

Step 2: 回路 C の各配線をベクトル表現に変形し，集合 W とする．

Step 3: $i = 1$ とする．

Step 4: $a_i = 1$ であるベクトルに注目し，a_{i+1} から a_n まで値が全て 0 になるベクトルを集合 W から探す．存在しなければ $x_i = 1$ とし，Step6 の処理を行う．

Step 5: Step 4 で見つけた各ベクトルの $(a_1, \ldots, a_i)$ と $(x_1, \ldots, x_i)$ の内積が 1 となるほうが多くなるように x_i の値を決め，内積が 1 となるベクトルを集合 W から削除する．

Step 6: $i \neq n$ ならば $i = i + 1$ とし，Step4 の処理へ戻る．

Step 7: 検査入力集合 T に，$(x_1, x_2, \ldots, x_n)$ を加える．

Step 8: 集合 W が空集合でなければ，Step3 に戻り，空集合ならば集合 W を出力する．

ただし，検査入力を生成する際，x_i の値が 1 と 0 の値のどちらでも良い場合は 1 を x_i の値としている．

アルゴリズム TESTSET(C) によって生成される T が完全な検査入力集合であるかを証明する．

定理 5 T は C に対する完全な検査入力集合であり，$|T| \leq \log(n+g) + 1$ である．

証明: まず，検査入力 $(0, 0, \ldots, 0)$ を検査入力集合 T に加えることで，全ての配線の値が 0 の場合を得る．検査入力の各ビットは，半分以上の配線の値を 1 になるように検査入力を決める．配線の値が 1 になるベクトル集合以外の残りのベクトル集合についてさらに処理を実行する．配線の数は常に半分以下になっていくので，やがて集合 W は空集合となる．空集合になった場合，全てのベクトルが 1 になる検査入力を得たことになる．よって T は C にとっての完全な検査入力集合となる．

このとき検査終了となる配線の数は $n + g$ 以下なので，検査入力集合 T の大きさは $\log(n+g)+1$ で収まり，$|T| \leq \log(n+g)+1$ となる． ■

定理 6 アルゴリズム TESTSET(C) の時間計算量は $O(n(n+g))$ である．

参考文献

[1] C. Bennett. Logical reversibility of computation. *IBM Journal of Research and Development*, 17:525–532, 1971.

[2] E. Fredkin and T. Toffoli. Conservative logic. *International Journal of Theoretical Physics*, 21, 1982.

[3] Hayes.J. Patel.K. and Markov.I. Fault testing for reversible circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 23.

[4] Tabei.K. and Yamada.T. On generating test sets for reversible circuits. *Computer Engineering and Systems 2009 ICCES 2009.International Conference*, pages 94–99, 2009.