設計自動化　59－13
（1991．10．9）

正則時相論理を用いた二重系照合回路のフェールセーフ性の形式的検証

川久保和雄　　平石裕実

福山大学工学部　　京都産業大学工学部

あらまし　多重系構成における照合回路などのようにフェールセーフ性などの耐故障性が要求される回路において、その性質を満足していることを検証することが厳密には必要である。本稿では順序機械のフェールセーフ性が入出力系列の関係で記述できることに着目し、正則時相論理を利用した形式的検証を提案する。具体的な例として二重系照合回路の検証を行った結果、フェールセーフ性の性質を比較的容易に記述することができ、十分実用的な時間で検証可能であることが確認された。この手法を一般化することにより、耐故障性の他の諸性質の検証にも利用することが可能であると考えられる。

Formal Verification of Fail-Safeness of a Comparator for Redundant System Using Regular Temporal Logic

Kazuo KAWAKUBO

Faculty of Engineering
Fukuyama University

1,Gakuen-cho,Fukuyama-shi,
Hiroshima,729-02,Japan

Hiromi HIRAISHI

Faculty of Engineering
Kyoto Sangyo University

Kamigamo-Motoyama,
Kita-ku,Kyoto,603,Japan

Abstract　It is necessary to verify that circuits which are required to have fault-tolerance including fail-safeness surely satisfy those conditions. In this paper we propose a method of formal verification of fail-safeness of sequential machines using regular temporal logic. We use a comparator for redundant system as an example to illustrate the verification of fail-safeness. In this example we present that it is rather easy to describe fail-safeness in form of input-output sequences, and that it takes not so much time to verify fail-safeness on Sun-3/50 workstation.

1. まえがき

システムの信頼性や安全性の向上を目的とした構成の一つに、モジュールを多重化し、多数決により故障をマスクする多重系構成がある[1]。多重系構成では、故障がマスクされたまま多重故障に遷移することを防ぐため、一般にモジュール同士、またはモジュールと多数決回路からの出力を比較して不一致検出によって故障を検知する照合回路が設けられる。これによって故障が検知されたモジュールは、多数決から排除されるなどの処置がとられる。この場合、照合回路自体の故障が原因でモジュール間の不一致を見逃すことのないよう、照合回路をセルフチェッキング性やフェールセーフ性などの耐故障性を満たす構成にすることが要求される。照合回路に限らず、それらの耐故障性を持つように設計されるべき回路については、厳密にはさらに、実際にそれらの性質を満足することを検証することが必要である。

耐故障性の検証の方法としては、内部の信号線に縮退故障を注入して論理シミュレーションを行う方法などが考えられる。しかしシミュレーションでは入力パターンの制約上、すべての場合を網羅することは困難である。一方、一般の論理設計の検証では、論理シミュレーションに対して、時相論理などの論理体系を用いて設計の正しさを証明する形式的検証のアプローチが研究されている。本論文ではそれらのアプローチと同様な考えに基づき、時相論理の一体系である正則集合と表現等価な正則時相論理を利用した耐故障性の形式的検証を提案する。この方法では、回路の満たすべき耐故障性を入出力系列の関係の形で正則時相論理式で記述し、設計された順序機械の可能な動作系列に対してその正則時相論理式が真であることを確かめることにより、回路の耐故障性を形式的に検証する。時相論理などを利用した論理設計の形式的検証は、仕様の記述が容易ではないので実用的には難しい面があるが、耐故障性の形式的検証では記述すべき仕様が類型的であるので、実用的に適していると考えられる。ここでは具体的な例として、フェールセーフ性を満足するように設計された二重系の照合回路について、正則時相論理による形式的検証の方法、及び実際にモデルチェックプログラムを用いて検証を行った結果について述べる。なお、この手法を一般化することにより、耐故障性の他の諸性質の検証にも利用することが可能であると考えられる。

以下、2章では前提として順序回路に対するフェールセーフ性の定義を述べた後、具体的に検証の対象とするフェールセーフ二重系照合回路について説明する。3章では正則時相論理の論理設計の形式的検証への応用について、まず正則時相論理の定義、続いてそれを利用した順序機械の設計検証の手順について述べる。4章ではこれをフェールセーフ性の形式的検証に応用する場合の方法を、照合回路を例にとりながら具体的に述べ、5章では実際にモデルチェックプログラムを利用して検証を行った結果を示す。

2. 二重系照合回路とフェールセーフ性

2.1 定義

ここで対象としているフェールセーフ性は一般的には、「故障が発生した場合に必ず安全側に動作し、誤った危険側の出力は出さない性質」といわれているものである。これを形式的に定義すると、組合せ回路に関するフェールセーフ性の定義は次のように与えられる。

［定義1］ 出力符号語集合の内、安全側の出力符号語集合 O_s をあらかじめ定め、故障集合 F に属する任意の故障に対して、入力符号語集合の中のいかなる符号語に対しても正常時と同じ出力符号語または O_s 内の符号語を出力する場合、この回路はフェールセーフであるという。 □

ここでは例にとった照合回路が順序回路であるので、定義1を順序回路に拡張する。定義1の中の入出力の「符号語」を「系列」に置き換えると、順序回路については次のように定義できる。

［定義2］ 出力系列集合の内、安全側の出力系列集合 O_s をあらかじめ定め、故障集合 F に属する任意の故障に対して、入力系列集合の中のいかなる系列に対しても正常時と同じ出力系列または O_s 内の系列を出力する場合、この回路はフェールセーフであるという。 □

2.2 二重系照合回路

ここで具体的な例として検証の対象とするのは、クロックレベルで完全に同期して動作する2個のモジュールからの出力の一致・不一致を判定する二重系照合回路[2]である（図1）。この照合回路は本来多数決により故障をマスクする多重系構成において、故障がマスクされたまま多重故障に遷移することを防ぐため、2個のモジュールからの出力を比較して不一致検出によって故障を検知することを目的に設けられている。これによって故障が検知されたモジュールは、多数決から排除されるなどの処置がとられる。従って多重系構成の中で重要な機能を有している回路であるので、照合回路自体の故障が原因でモジュール間の不一致を見逃すことのないよう、フェールセーフ性を満足するように要求されている。すなわち、照合回路内に故障が発生した場合、誤った一致情報を出力しないように設計されている。

図1で2ビット双方向シフトレジスタの各ビットには

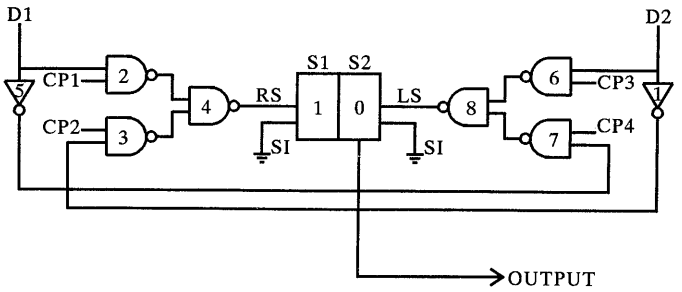

図1　二重系照合回路図

$S1 = 1$, $S2 = 0$ が初期値として与えられている。この2ビットが通常セルフチェッキングシステムで用いられる2線式のチェッカに相当するが、この回路の出力は1本の出力線 $S2$ 上に得られる交番出力による時間冗長方式をとっている。照合はある時間幅を持った比較サイクル単位で行われる。1比較サイクルの中で2系からの照合入力 $D1$, $D2$ が一致している場合は、順に発生するクロック $CP1$〜$CP4$ の中の二つに同期してシフトレジスタが左右に各1度ずつシフトされる。どの二つに同期するかは、$D1$, $D2$ の値による。この動作にともない $S2$ から、0と1の交番出力が得られる。また二つの照合入力間に不一致がある場合は連続して同方向のシフトが行われるようになっており、その結果、シフトレジスタの両ビットはともに0になり以後 S2 からの出力は0が持続する非交番出力となる。したがって1比較サイクルでも不一致があれば、その後不一致発生情報を保持することができる（図2）。これはいわゆるセルフチェッキングチェッカにおける誤り表示に相当する。

3．正則時相論理を利用した順序機械の設計検証

3.1　正則時相論理の定義

組合せ論理回路に対応する論理体系として命題論理があるが、順序回路、あるいは一般的に順序機械や有限オートマトンを扱うためには、時間の概念を扱うことができる時相論理などの論理体系が必要である。従来からいくつかの時相論理体系の研究やそれを利用した設計検証システムの開発が行われてきているが、これらの中で順序機械の動作系列を記述するのに適したものとして、有限オートマトンと等価な表現能力を持つ論理体系である正則時相論理[3][4]がある。正則時相論理は通常の命題論理に対して、時間の概念を扱う演算子として「次の時刻」、「次の区間」、「繰り返し」を意味する三つの時相論理演算子「○」、「:」、「[:]」を追加して構成したものである。正則時相論理は正則集合と表現等価であるため、任意の有限オートマトンの仕様を動作系列（入出力系列）の形で完全に記述することが可能である。次に正則時相論理式の定義を示す。

［定義3］　AP を原始命題の集合とする。このとき、次の生成規則1－3の有限回の適用により得られる式を正則時相論理式という。

1. $p \in AP$ のとき、p は正則時相論理式である。
2. η が正則時相論理式の時、（$\neg\eta$）、（$\bigcirc\eta$）、（$[:]\eta$）は正則時相論理式である。
3. η、ξ が正則時相論理式の時、（$\eta \vee \xi$）、（$\eta : \xi$）は正則時相論理式である。　□

ここでの「$\bigcirc\eta$」は次の時刻から始まる系列に対して η が成立することを意味し、「$\eta : \xi$」は系列の前半で η が成立し後半で ξ が成立することを意味し、「$[:]\eta$」は η が繰り返し成立することを意味している。またこれらから、系列の長さが1であることを意味する「$LEN1$」、現時刻以降いつか ξ が成立することを意味する「$\Diamond$」、及び現時刻以降常に ξ が成立することを意味する「$\Box$」を導くことができる。以下ではこの他、「$\wedge$」、「$\Rightarrow$」、「$=$」、「V_T」、「V_F」の記号で、各々通常の命題論理の「論理積」、「含意」、「等価」、「恒真式」、「恒偽式」を表し、単項演算子は二項演算子よりも優先順位が高いものとする。

なお正則時相論理式の真偽値を定義する領域をすべての長さ1以上の有限長語の集合とした場合、これを ε フリー有限正則時相論理という。ここでは有限長の動作系列を扱うので、この ε フリー有限正則時相論理式で仕様を記述するものとする。以下、ε フリー有限正則時相論理を単に RTL と書く。

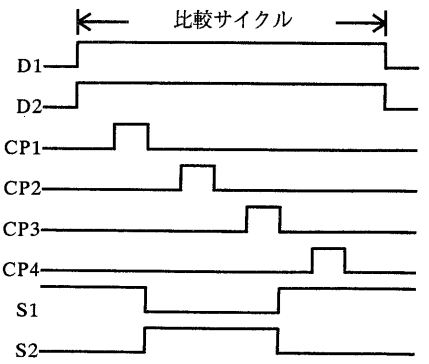

図2　比較サイクルのタイミングチャート

3.2 正則時相論理を利用した論理設計の形式的検証の手順

εフリー有限正則時相論理を利用した論理設計の形式的検証は、次のような手順で行うことになる。

(1) 設計対象の回路を順序機械で表現する。
順序機械は決定性の Mealy 型あるいは Moore 型で記述する。

(2) 設計仕様を RTL 式で記述する。
設計仕様は、設計対象の順序機械の可能な動作系列の集合として与えられるものとする。ここでは任意の長さの有限動作系列を考える。回路が n ビットの入力信号 $X = \{x_1, x_2, \cdots, x_n\}$ と m ビットの出力信号 $Z = \{z_1, z_2, \cdots, z_m\}$ を持つものとし、入力信号 x_i に対して $x_i = 1$ のときに限り真となる原始命題 p_{xi} $(1 \leqq i \leqq n)$ と出力信号 z_j に対して $z_j = 1$ のときに限り真となる原始命題 p_{zj} $(1 \leqq j \leqq m)$ を用いて、設計対象の順序機械において可能な任意の長さの有限動作系列の集合を RTL 式で記述する。

(3) 設計対象の順序機械のすべての可能な有限長の動作系列に対して、仕様のすべての RTL 式が真となることを確かめる。

可能なすべての動作系列に対しての RTL 式の真偽判定は文献 [4] で示されたモデルチェックアルゴリズムにより可能である。

4. 順序機械のフェールセーフ性の形式的検証

前節で述べた論理設計検証と同様な考えに基づき、順序機械のフェールセーフ性の形式的検証を行うためには、まず論理設計検証と同様に対象の回路を順序機械で表現し、その上で要求される回路のフェールセーフ性を満足するような動作系列の集合を、RTL 式で記述する。論理設計検証での回路の仕様の記述と異なり、フェールセーフ性に直接関連する動作系列の集合のみを記述すればよい。フェールセーフ性を満足する動作系列とは、定義 2 を具体的な入出力系列で表現したものである。すなわち故障集合 F に属するすべての故障について、それの存在を仮定した上で可能なすべての有限長の入力系列を与えた場合に、正常な出力系列あるいは安全側の出力系列集合 O_s 内の出力系列のみを出力することを RTL 式で記述することになる。ここで故障集合 F に属する故障 f_i $(1 \leqq i \leqq n)$ が存在する場合の回路の仕様を C_{fi}、回路への入力系列を I_j $(1 \leqq j \leqq m)$、故障のない場合のその入力系列に対応した出力系列を O_{Ij}、安全側の出力系列集合 O_s に属する出力系列を O_{sk} $(1 \leqq k \leqq r)$ とすると、上に述べたことは次の式で表すことができる。

$\forall f_i \in F$、$\forall I_j$ について

$$C_{fi} \wedge I_j \Rightarrow O_{Ij} \vee O_{s1} \vee O_{s2} \vee \cdots \vee O_{sr} \quad (1)$$

これらの RTL 式がすべて真となることが示されれば、この順序機械がフェールセーフであることが検証されることになる。以下では前述した二重系照合回路を対象として、具体的にフェールセーフ性を検証する手順について述べる。

4.1 順序機械の表現

この照合回路の入力信号は、照合の対象となる 2 系からの入力信号 $D1$,D2 とシフトレジスタのシフトパルスのタイミングを生成する 4 相のクロック信号 $CP1 \sim CP4$ の六つであり、出力信号はシフトレジスタの 1 ビット $S2$ である。また内部信号として、シフトレジスタへの右シフトパルスと左シフトパルスの RS と LS の二つを考える。シフトレジスタはネガティブエッジトリガで動作するとする。RS と LS はパルス幅を持ったパルス信号と考え、それぞれの状態と $S1$,S2 の状態を組み合わせて 10 状態の Moore 型順序機械で記述してある。この順序機械の入力としては照合回路の六つの入力信号から組合せ回路により生成される RS と LS を考える。

なおここではシフトレジスタ自体の故障は考えないものとする。もちろんこの次の段階では、シフトレジスタ内部についても検証を行う必要がある。すなわち回路全体を階層的に考え、各レベルごとに検証を行うと効率がよいと考えられる。

4.2 正則時相論理による仕様の記述

4.2.1 動作系列によるフェールセーフ性の記述

次にフェールセーフ性を表現する動作系列の集合などを仕様の形で RTL 式で記述する。まず回路の入出力を有限オートマトンの入力系列及び出力系列とみなす。入力アルファベット Σ は $D1$, $D2$, $CP1 \sim CP4$ からなる 6 ビットの入力ベクトルの集合であり、入力系列集合 Σ^+ は Σ 上のすべての長さ 1 以上の有限長の系列からなる集合である。一方出力アルファベット Γ は信号線 $S1$ と $S2$ からなる 2 ビットの出力ベクトルの集合であり、出力系列集合 Γ^+ は Γ 上のすべての長さ 1 以上の有限長の系列からなる集合である。

これらをもとにして可能なすべての有限長の入出力系列を記述する。対象の照合回路について具体的に記述したものを図 3 に示す。可能な入力系列とは Σ^+ の中で次の二つの入力制約を満たす系列である。一つは「$CP1 \sim CP4$ がどの二つも同時に1になる期間はない」ことを入力ベクトルの制約としたものが $c0 \sim c4$ である。もう一つ

$$
\begin{aligned}
c0 &\triangleq \neg CP1 \wedge \neg CP2 \wedge \neg CP3 \wedge \neg CP4\\
c1 &\triangleq \quad CP1 \wedge \neg CP2 \wedge \neg CP3 \wedge \neg CP4\\
c2 &\triangleq \neg CP1 \wedge \quad CP2 \wedge \neg CP3 \wedge \neg CP4\\
c3 &\triangleq \neg CP1 \wedge \neg CP2 \wedge \quad CP3 \wedge \neg CP4\\
c4 &\triangleq \neg CP1 \wedge \neg CP2 \wedge \neg CP3 \wedge \quad CP4\\
cspec &\triangleq \Box(c0):\Box(c1):\Box(c0):\Box(c2):\Box(c0):\Box(c3):\Box(c0):\Box(c4):\Box(c0):\Box(c0)\\
fix &\triangleq \Box(TRUE)\\
g1 &\triangleq \neg D1\\
g2 &\triangleq \neg(D1 \wedge CP1)\\
g3 &\triangleq \neg(g1 \wedge CP2)\\
g4 &\triangleq \neg(g2 \wedge g3)\\
g5 &\triangleq TRUE\\
g6 &\triangleq \neg(D2 \wedge CP3)\\
g7 &\triangleq \neg(g5 \wedge CP4)\\
g8 &\triangleq \neg(g6 \wedge g7)\\
asrl &\triangleq \Box((RS = g4) \wedge (LS = g8))\\
a\_cond &\triangleq cspec \wedge (\Box(D1 \wedge D2) \vee \Box(\neg D1 \wedge \neg D2))\\
a\_rslt &\triangleq cspec \wedge (\Box(S1 \wedge \neg S2) : \Box(\neg S1 \wedge S2) : \Box(\neg S2 \wedge S1))\\
a\_rslt\_1 &\triangleq cspec \wedge (\Box(S1 \wedge \neg S2) : \Box(\neg S1 \wedge S2))\\
a\_rslt\_2 &\triangleq cspec \wedge (\Box(\neg S1 \wedge S2) : \Box(S1 \wedge \neg S2))\\
b\_cond &\triangleq cspec \wedge (\Box(D1 \wedge \neg D2) \vee \Box(\neg D1 \wedge D2))\\
b\_rslt &\triangleq cspec \wedge (\Box(\neg S2) \vee \Box(S2)) \vee (\neg S1 \wedge \neg S2)\\
ab\_cond &\triangleq (a\_cond : b\_cond) \vee b\_cond\\
cond\_1 &\triangleq a\_cond : a\_cond\\
cond\_2 &\triangleq a\_cond : b\_cond\\
as1 &\triangleq (fix \wedge \boxdot(a\_cond) \wedge asrl) \Rightarrow\\
&\quad (\boxdot(a\_rslt \vee a\_rslt\_1 \vee a\_rslt\_2) \vee \Diamond(b\_rslt))\\
as2 &\triangleq (fix \wedge (ab\_cond : \boxdot(cond\_1 \vee cond\_2 \vee b\_cond)) \wedge asrl) \Rightarrow\\
&\quad \Diamond(b\_rslt)\\
assertion &\triangleq as1 \wedge as2
\end{aligned}
$$

図3　照合回路のフェールセーフ性の仕様

は「1比較サイクルの中で $CP1$〜$CP4$ がこの順番に1度ずつ発生する」ことで系列に制約を与えたものが $cspec$ になる。従って $cspec$ で定義された区間が1比較サイクルとなる。ここではクロックパルスの幅は特に与えていないが、これは仕様を動作系列で表現しているため任意のパルス幅を扱えるからである。また「$D1$, $D2$ が1比較サイクル内ではともに変化しない」という制約は $D1 = D2$ の場合が a_cond、$D1 \neq D2$ の場合が b_cond で表されている。結局これらの入力制約をすべて満たす入力系列集合 I は、1比較サイクル単位での部分系列である a_cond と b_cond の有限回（1回以上）のすべての繰り返しでできる系列の集合であり、Σ^+の部分集合である。なお、$D1$, $D2$, $CP1$〜$CP4$ はいずれも対応する信号線の値が1の時に真になる原始命題として与えている。

出力系列の記述ではΓ^+の中から、交番出力と非交番出力を1比較サイクル単位の部分系列として定義する。交番出力は1比較サイクルの中で、信号線の値が1の時に真になる原始命題の組 ($S1$, $S2$) の値が（真，偽）、（偽，真）、（真，偽）の順で繰り返される部分系列として定義する。この変化をそれぞれの区間の連接で表したものと1比較サイクルを表す $cspec$ との論理積で表現したものが図3の a_rslt である。連接表現の中で□を用いているが、これはその区間の中では $S1$ 及び $S2$ の値が一定であることを示している。また非交番出力は図3の b_rslt のように、出力線 $S2$ の値が1比較サイクルの中で変化しない、すなわち常に真か常に偽である部分系列として定義する。但し、定義の中では、さらに $S1$ と $S2$ が同時に偽となる状態も含めている。これはシフトレジスタの両ビットが0になった状態で次の比較サイクル以降は交番出力は出ないことを示している。これを定義に含めているのは、有限長の動作系列の最後にこの状態が来る系列に対して RTL 式を真にする必要があるからである。

この回路の場合、1比較サイクル単位で照合入力と4クロックパルスが与えられると、照合入力 ($D1$, $D2$) の一致または不一致に従って順序機械の出力 $S2$ から交番出力の部分系列 a_rslt、または非交番出力の部分系列 b_rslt が出力される。また、一度でも照合入力の不一致の比較サイクルがあり b_rslt が発生すれば、それ以後は照合入力の一致不一致にかかわらず b_rslt が繰り返され、不一致発生情報は保持される。従って b_rslt が2入力の不一致を表しているので、ある時刻以降有限長の系列の最後まで b_rslt が繰り返される系列がΓ^+の中での安全側の出力系列と考えられる。従ってここではその条件を満たす出力系列の集合を安全側の出力系列集合 O_s に定める。この回路のフェールセーフ性を検証するためには、定義2に従って、故障集合 F に属する故障が存在する場合に、I の中のすべての入力系列に対してそれに対応する正常な出力系列あるいは O_s 内の出力系列のみを出力することを検証すればよい。すなわち (1) 式に対応する RTL 式を記述して、それらがすべて真になることを確かめればよい。

I の中の入力系列は前述のように1比較サイクル単位の部分系列 a_cond と b_cond の有限回の繰り返しからなる系列であるが、その中で照合入力が一致している比較サイクルの部分系列 a_cond の繰り返しだけからなる入力系列に対しては、それに対応する正常な出力系列は交番出力の部分系列 a_rslt の繰り返しだけからなる系列である。一方それ以外の可能な入力系列、すなわち照合

入力不一致の部分系列 b_cond が少なくとも1回は含まれる系列に対しては対応する正常な出力系列は非交番出力の部分系列 b_rslt が系列の最後まで繰り返される系列であり、上記の O_s 内の系列と一致する。これを入出力系列の関係で記述したのが図3の $as1$ 及び $as2$ になる。$as1$ は「照合入力が一致している比較サイクルが繰り返されるならば、出力系列は交番出力の部分系列が繰り返されるか、またはいつかは非交番出力になる」ことを表現しており、$as2$ は「照合入力が不一致の比較サイクルが1回でも存在するならば、出力系列はいつかは非交番出力の比較サイクルが持続する状態になる」ことを表現している。この中で「いつか」という表現を用いているのは、回路の性質上入力の不一致発生から非交番出力の比較サイクルまで遅延があるため、その入力と出力間の遅延を吸収するためである。また $as2$ では、その遅延を考慮して有限長の入力系列の最後が特定のパターン $(b\_cond : a\_cond)$ で終わるものを除外するようにしてある。このようにRTLでは対象が有限長の動作系列であるため、系列の最後の部分を考慮する必要がある場合がある。なお、図3の記述ではさらに故障が全区間固定されていることを表現する fix が論理積の形で含まれている。以上から、この回路の満たすべき性質は $as1$ と $as2$ の論理積である $assertion$ で表現できる。

4.2.2 故障と組合せ回路部分の記述

回路のフェールセーフ性を記述するためには、動作系列の他にその前提となる故障集合の要素を記述する必要がある。ここでは故障集合 F の要素は、入力信号から内部信号の RS と LS を生成する組合せ回路部分のすべてのゲートの信号線単位の単一縮退故障としている。図3で $g1$〜$g8$ が回路のゲート間の関係及び入出力との関係を命題論理で記述したものであり、それぞれ図1のゲート1〜8に対応している。また $asrl$ は順序機械の入力である RS と LS をゲート4と8の出力 $g4$ と $g8$ で定義していることを示している。

縮退故障は、各ゲートの論理式を故障によって変化した機能を表す論理式で書き換えることによって記述する。例えば図1のゲート5の出力線に1縮退故障を仮定する場合は、常に真である原始命題 $TRUE$ を導入し、

$$g5 = TRUE$$

と書き換えることにより表現できる（図3）。また、入力線の1本に1縮退故障を仮定する場合は、それによって変化した後の機能を論理式で記述することになる。

フェールセーフ性の検証には故障集合のすべての要素についてそれぞれ検証することが必要である。この回路では等価な縮退故障（NAND素子の入力線0縮退故障と出力線1縮退故障など）を除いて、28種類の縮退故障が考えられる。これらのそれぞれに対応してゲート部分を書き換えた28種類の仕様を記述し検証することになる。ただし、多種類の仕様を個々に作成する煩雑さを避けるため、故障ゲートや故障の種類（信号線、縮退故障の種類）を符号化して記述する方法がある[5]。この方法を用いると、この回路の場合ゲート数が8であり、1ゲートあたりの故障の種類はNANDゲートの出力線の0と1の縮退故障、入力線1と2の1縮退故障の4種類があるので5ビットで符号化できる。符号の各ビットを原始命題で与え、真の値を持つ原始命題の組み合わせでゲートと故障の種類が選択されるように各ゲートの仕様を記述することにより、回路内のすべての単一縮退故障を一つの仕様で同時に検証することができる。これはデマルチプレクサを内蔵した等価回路を構成して、各ゲートごとに正常なゲートと縮退故障によって変化した機能をもつゲートからの出力を、原始命題で与えられる符号で選択されるようにしたものと考えることができる。この場合、符号の各ビットを表す原始命題は、動作系列の全区間において一定値をとることを条件としておくことが必要である。

5. 検証結果

実際に ε フリー有限正則時相論理式のモデルチェックプログラムを利用して上記の検証をsun3/50で実行した結果を表1に示す。この表から、いくつかの場合においてこの回路はフェールセーフ性を満足しないことがわかる。フェールセーフ性を満足しない入出力系列は大別して2種類のパターンに分類され、表1のタイプに示している。タイプ1は例えば図4のような入出力系列であり、ゲート1の出力線に0縮退故障を仮定したとき、照合入力が $D1 = D2 = 1$ の場合及び、$D1 = 0$, $D2 = 1$ の場合は、回路は正常時と同じ出力系列を出力する。しかし、$D1 = 1$, $D2 = 0$ であれば RS のみが発生し、$D1 = D2 = 0$ の場合は LS のみが発生する。従ってこの照合入力の系列がこの順序で連続して発生した場合には、2比較サイクルにわたって RS と LS が連続して各1回ずつ現れるため、これ以降も交番出力が持続し、不一致があったにもかかわらず O_s 内の出力系列にならない。

一方タイプ2は図5のような入出力系列であり、ゲート6の入力線2に1縮退故障を仮定したとき、$D1 = 0$, $D2 = 1$ の場合、RS は発生せず LS は1のまま持続する。続いて $D1 = D2 = 1$ に変化すると、RS のみが発生し LS は1が持続したままになるので、右方向のシフトが1回だけ行われる。さらに次の比較サイクルで $D1 = D2 = 0$ に変化すると、比較サイクルの最初で LS が0に変化するためこの立ち下がりで左方向のシフトが

ゲート	縮退故障		結果	時間（秒）	タイプ
$g1$	出力	s-a-0	Fail	13.2	1
		s-a-1	O.K.	30.3	
$g2$	出力	s-a-0	O.K.	103.6	
		s-a-1	Fail	24.8	1
	入力	#1	O.K.	41.4	
		#2	O.K.	160.1	
$g3$	出力	s-a-0	O.K.	100.4	
		s-a-1	Fail	12.4	1
	入力	#1	O.K.	41.9	
		#2	O.K.	332.2	
$g4$	出力	s-a-0	O.K.	104.4	
		s-a-1	O.K.	102.7	
	入力	#1	Fail	32.0	1
		#2	Fail	16.2	1
$g5$	出力	s-a-0	Fail	11.6	1
		s-a-1	O.K.	33.7	
$g6$	出力	s-a-0	O.K.	208.6	
		s-a-1	Fail	48.7	1
	入力	#1	O.K.	44.7	
		#2	Fail	28.7	2
$g7$	出力	s-a-0	O.K.	208.9	
		s-a-1	Fail	11.7	1
	入力	#1	O.K.	46.1	
		#2	Fail	38.5	2
$g8$	出力	s-a-0	O.K.	221.8	
		s-a-1	O.K.	205.2	
	入力	#1	Fail	65.5	1
		#2	Fail	12.9	1

表1　検証結果

行われ初期状態に戻る。従ってその後のサイクルで $D1 = D2 = 0$ のまま変化がなければ交番出力が持続することになり、やはり O_s 内の出力系列にならず、不一致発生情報が失われることになる。

これらの例の場合は、ある特定の順序の入力系列が発生する場合に現象が現れるのであるが、このような特定の順序に依存した現象を抽出するためには時系列に対する検証が必要であり、一般には論理シミュレーションでは検出しにくい。入出力系列を考えた形式的検証で行うのが適しているケースと考えられる。

なお、いずれの場合も現象の発生確率は非常に小さいと考えられる。例えば図4の現象は、ゲート1に縮退故障が発生した後、2照合入力に不一致が現れるまでに一度も $D1 = D2 = 0$ の状態が発生しないという場合に発生する。なぜなら、縮退故障発生後一度でも $D1 = D2 = 0$ の状態になれば、そのサイクルでは LS のみ発生し、その直後のサイクルで、シフトレジスタ内から「1」が失われることになり、その後は交番出力は発生しないからである。実際に、前述のフェールセーフ性の表現で、縮退故障が発生した後照合入力が不一致になるまでの間、比

```
D1    1111111111111 000000000000000 111111111111111
D2    0000000000000 000000000000000 000000000000000

CP1   0100000000000 001000000000000 001000000000000
CP2   0000100000000 000001000000000 000001000000000
CP3   0000000100000 000000001000000 000000001000000
CP4   0000000000100 000000000001000 000000000000100

RS    0100000000000 000000000000000 001000000000000
LS    0000000000000 000000000001000 000000000000000

S1    1110000000000 000000000000011 111100000000000
S2    0001111111111 111111111111100 000011111111111
```

図4　入出力系列の例（タイプ1）

```
D1    0000000000000 0000000000000000 111111111111111 000000000000000
D2    0000000000000 1111111111111111 111111111111111 000000000000000

CP1   0100000000000 0010000000000000 001000000000000 001000000000000
CP2   0000100000000 0000010000000000 000001000000000 000001000000000
CP3   0000000100000 0000000010000000 000000001000000 000000001000000
CP4   0000000000100 0000000000010000 000000000000100 000000000000100

RS    0000100000000 0000000000000000 0010000000000000 000001000000000
LS    0000000000100 1111111111111111 1111111111111111 000000000000100

S1    1111110000001 1111111111111111 1111000000000000 011111100000001
S2    0000001111110 0000000000000000 0000111111111111 100000011111110
```

図5　入出力系列の例（タイプ2）

較サイクル単位で $D1$, $D2$ にすべての変化パターンが出現するという条件を追加して検証した。その条件を記述したのが図6で、結果はすべての故障に対してこの条件を満足することがわかった。このように、入力系列にさらに条件を追加して検証を行うことにより、現実的にどの程度のレベルの条件のもとでフェールセーフ性が確保されるかを容易に確認することができるのも、この方法での形式的検証の長所であるということができる。なお、表1から計算時間も実用的であり、特に、満足しない場合にそれを検出する時間は非常に短いことがわかる。

6. あとがき

順序機械のフェールセーフ性の性質が入出力系列の関係で表現できることに着目し、正則時相論理を利用して順序機械のフェールセーフ性を形式的に検証することを提案して、具体的な例として二重系照合回路の検証を行った。その結果、フェールセーフ性の性質を比較的容易に仕様の形で記述することができ、十分実用的な時間で検証可能であることがわかった。また例に用いた照合回路はフェールセーフ性を満足しないが、入力系列のパターンの出現の条件を追加すると、満足することが示された。正則時相論理は有限オートマトンと等価な表現能力を持つ論理体系であり、すでに順序機械の設計検証への応用が研究されている。同様にフェールセーフ性を含む耐故障性の形式的検証に有効であると考えられる。今後、耐故障性の他の諸性質についても、正則時相論理を応用した形式的検証の手法を検討していく予定である。また、故障集合についても縮退固定故障のみでなく間欠故障などを対象とした検証も進めている。

$$
\begin{aligned}
c0 &\triangleq \neg CP1 \wedge \neg CP2 \wedge \neg CP3 \wedge \neg CP4\\
c1 &\triangleq CP1 \wedge \neg CP2 \wedge \neg CP3 \wedge \neg CP4\\
c2 &\triangleq \neg CP1 \wedge CP2 \wedge \neg CP3 \wedge \neg CP4\\
c3 &\triangleq \neg CP1 \wedge \neg CP2 \wedge CP3 \wedge \neg CP4\\
c4 &\triangleq \neg CP1 \wedge \neg CP2 \wedge \neg CP3 \wedge CP4\\
cspec &\triangleq \Box(c0):\Box(c1):\Box(c0):\Box(c2):\Box(c0):\Box(c3):\Box(c0):\Box(c4):\Box(c0):\Box(c0)\\
fix &\triangleq \Box(TRUE)\\
g1 &\triangleq \neg D2\\
g2 &\triangleq \neg(D1 \wedge CP1)\\
g3 &\triangleq \neg(g1 \wedge CP2)\\
g4 &\triangleq \neg(g2 \wedge g3)\\
g5 &\triangleq TRUE\\
g6 &\triangleq \neg(D2 \wedge CP3)\\
g7 &\triangleq \neg(g5 \wedge CP4)\\
g8 &\triangleq \neg(g6 \wedge g7)\\
asrl &\triangleq \Box((RS = g4) \wedge (LS = g8))\\
a\_cond &\triangleq cspec \wedge (\Box(D1 \wedge D2) \vee \Box(\neg D1 \wedge \neg D2))\\
a\_1 &\triangleq cspec \wedge (\Box(D1 \wedge D2)\\
a\_0 &\triangleq cspec \wedge (\Box(\neg D1 \wedge \neg D2)\\
a\_10 &\triangleq \boxdot(a\_1) : a\_1 : \boxdot(a\_0) : a\_0\\
a\_01 &\triangleq \boxdot(a\_0) : a\_0 : \boxdot(a\_1) : a\_1\\
b\_cond &\triangleq cspec \wedge (\Box(D1 \wedge \neg D2) \vee \Box(\neg D1 \wedge D2))\\
b\_rslt &\triangleq cspec \wedge (\Box(\neg S2) \vee \Box(S2)) \vee (\neg S1 \wedge \neg S2)\\
assertion &\triangleq (fix \wedge (\boxdot(a\_cond) : (a\_10 \vee a\_01) : \boxdot(a\_cond) : b\_cond :\\
&\qquad \boxdot(a\_cond \vee b\_cond)) \wedge asrl) \Rightarrow \Diamond(b\_rslt)
\end{aligned}
$$

図6　入力パターンを追加した場合の仕様

謝辞　日頃ご指導いただく京都大学矢島脩三教授、ならびに検証プログラムを作成された藤井寛氏に深く感謝致します。

参考文献

[1] D.P.Siewiorek and R.S.Swarz: *The Theory and Practice of Reliable System Design*, Digital Press (1982)

[2] K.Kawakubo, H.Nakamura and I.Okumura: The Architecture of a Fail-Safe and Fault-Tolerant Computer for Railway Signalling Device, *Proc. 10th Int. Symp. Fault-Tolerant Computing*, , pp.372-374 (1980)

[3] 平石、濱口、藤井、矢島：有限オートマトンと表現等価な正則時相論理とその論理設計検証への応用,情報処理学会論文誌, Vol.31 No.7, pp.1134-1145 (1990)

[4] 藤井、平石、矢島：正則時相論理の直接モデル検査法を用いた順序機械の形式的検証, 電子情報通信学会技術研究報告, FTS90-14 (1990)

[5] N.Takahasi, N.Ishiura and S.Yajima: Fault Simulation for Multiple Faults Using Shared Binary Decision Diagrams, *Proc. Synthesis and Simulation Meeting and International Interchange*, pp.157-164 (1990)