数理解析研究所講究録
第140巻 1972年 336-352

多値フェイルセイフシステム

日本電信電話公社武蔵野電気通信研究所
高岡忠雄

1. はじめに

渡辺，高橋(1)によって提出されたフェイルセイフシステムの研究は，最初，入力，及び論理素子の出力が非対称に誤るとき，全システムの出力が非対称に誤るように論理回路を構成できるかという問題から出発した。安全側へ出力が非対称に誤ってもそれは許容される場合があるというのがフェイルセイフの言葉の由来である。その後の研究者達による結論を述べれば，実現するべき論理関数がユネイトであることが十分条件であり，また，論理関数がユネイトでない場合，それぞれ別の方向へ非対称に誤る入力および論理素子を用いシステムを二重化することによってフェイルセイフシステムを構成することができるということであった。一方，著者ら(2)が提唱したN-フェイルセイフシステム（別の著者(3)によって亜形フェイルセイフともいう）を二重系を用いて構成することにより，上記の古典的フェイルセイフシステムの理論を包含し得る。本稿では，このN-フェイルセイフの概念を一般の多値論理系に拡張し，多値論理関数を二値

非対称誤り素子および入力を用いて，フェイルセイフに実現するシステムの構成法について述べる。この議論は，二値論理の場合のN－フェイルセイフの概念を完全に含むことが判明する。

2. 多値論理関数のフェイルセイフ関数

定義1．m個の真理値からなる真理値集合Tを$T=\{t_0, \cdots, t_{m-1}\}$で定義する。$n$変数の$m$値論理関数とは，写像$f: T^n \to T$で定義される。変数を$x_1, \cdots, x_n$で表わし，関数を$f(x_1, \cdots, x_n)$で表わす。変数ベクトルを$\mathbf{x}=(x_1, \cdots, x_n)$で表わすことにより，関数を$f(\mathbf{x})$とも記す。

定義2．Tのすべての部分集合からなる集合（すなわちTのべき集合）から空集合をとり去ったものを$\tilde{T}$で表す。$\tilde{T}$の元の個数は2^m-1である。$x, y \in \tilde{T}$に対し，その大小関係$x \leq y$を，x, yがTの部分集合としてyがxを含むか，或いはxに等しいときで定義する。かくして，$\tilde{T}$はこの順序に関して半順序集合となる。また，各$t_i \in T$に対し，$\{t_i\}$とt_iを便宜上同一視する。

定義3．関数$f': \tilde{T}^n \to \tilde{T}$が関数$f: T^n \to T$のフェイルセイフ（FS）関数であるとは

$$\forall x \in T^n \quad f'(x) = f(x) \tag{1}$$

$$\forall x \in T^n, \forall x' \in \hat{T}^n \quad x \leq x' \Rightarrow f(x) \leq f'(x') \tag{2}$$

が成り立つときをいう。　ここに $x \leq x'$ はその要素ごとの大小関係による。

このFS関数の定義の意味はつぎの如くである。　すなわち，入力 x が T^n の範囲内にあるときは正しい入力であるから $f'(x)$ の出力値は正しく $f(x)$ の値と一致する。　入力の誤り $x \to x'$ は $x \in T^n$, $x' \in \hat{T}^n$ で $x \leq x'$ なるものに限る。このとき，$f'(x')$ の値を，$x \leq x'$, $x \in T^n$ なるすべての x に対する $f(x)$ の値を含むように，$\hat{T}$ の元でもって定義しようというわけである。

補題1．$x_1, \cdots, x_r$ をそれぞれ適当な次元の変数ベクトルとする。　$f_1(x_1), \cdots, f_r(x_r)$, $g(y_1, \cdots, y_r)$ がそれぞれ m 値論理関数で，$f_1'(x_1), \cdots, f_r'(x_r)$, $g'(y_1, \cdots, y_r)$ がそれぞれのFS関数であるとするとき，関数 $g'(f_1'(x_1), \cdots, f_r'(x_r))$ は $g(f_1(x_1), \cdots, f_r(x_r))$ のFS関数である。

証明．明らかである。

これによって，フェイルセイフシステムをカスケードに合成するとき，フェイルセイフ性が保存されることがわかる。

定義4．f のFS関数 f', f'' に対し，順序 $f' \leq f''$ を

$$f' \leq f'' \Leftrightarrow \forall x \in \tilde{T}^n \; f'(x) \leq f''(x) \qquad (3)$$

で定義する．

$x \in \tilde{T}^n$は入力情報の拡散を意味し，$f'(x)$ の値は出力の値の拡散を意味するから，出力が誤りでない限りにおいて，この出力における情報損失を最小にするようなFS関数が効率の観点から望ましい。それは(3)式の意味での順序における最小のFS関数を求めることである。

定義5．与えられたm値論理関数$f(x)$に対して，関数$\tilde{f}$: $\tilde{T}^n \rightarrow \tilde{T}$をつぎのように定義する。

$$\tilde{f}(x_1, \cdots, x_n) = \{f(a_1, \cdots, a_n) \mid a_1 \in x_1, \cdots, a_n \in x_n\} \quad (4)$$

補題2．$\tilde{f}$はfのFS関数である。

証明．条件(1)は明らかである。条件(2)については，

$$\forall x, \forall x \in \tilde{T}^n \; x \leq x' \Rightarrow \tilde{f}(x) \leq \tilde{f}(x')$$

が成り立つ。すなわち，$\tilde{f}(x)$は単調増大関数であり，したがって条件(2)をみたす。（証明終）

補題3．fの任意のFS関数f'に対して$\tilde{f} \leq f'$がなりたつ。

証明．(2)より

$$\forall y \in T,\ \forall x \in \tilde{T}^n \quad y \le x \Rightarrow f(y) \le f'(x)$$

である．このようなすべての $f(y)$ を集めた集合が $\tilde{f}(x)$ に他ならない。それ故

$$\forall x \in \tilde{T}^n \quad \tilde{f}(x) \le f'(x)$$

が成り立つ。（証明終）

$m=2$ の場合，著者らは集合 $\{0,1\}$ に N という名前をつけ，平山らは亜という名前をつけた。そして，情報損失最大の関数を向殿(4)はC形フェイルセイフ関数と呼んだ。否定，論理積，論理和に対する関数 $\tilde{f}$ をつぎの表に示しておく．

表 1.

x	0	1	N
$\tilde{f}$	1	0	N

否定

$x_1 \backslash x_2$	0	1	N
0	0	0	0
1	0	1	N
N	0	N	N

論理積

$x_1 \backslash x_2$	0	1	N
0	0	1	N
1	1	1	1
N	N	1	N

論理和

3. 関数の展開

本節では，関数を展開したとき，情報損失度がどのように変化するかについて考察する。 まず，$f(x)$ が

$$f(x) = F(f_1(x_1), \cdots, f_r(x_r)) \qquad (5)$$

$$x_1 \cup \cdots \cup x_r = x$$

という形式に展開できたものとする。 ここに，各 $f_i(x_i)$ および $F(y_1, \cdots, y_r)$ は m 値論理関数であり，記号"$\cup$"は各変数ベクトル x_i を集合とみなしてそれらの和集合をとることを意味する。 $\tilde{F}(\tilde{f}_1(x_1), \cdots, \tilde{f}_r(x_r))$ を簡単のため $\tilde{F}(x)$ と記す。

補題 1 および 3 より

補題 4. $\hat{F}(x)$ は $f(x)$ の FS 関数であり

$$\forall x \in \tilde{T}^n \quad \tilde{f}(x) \le \hat{F}(x) \qquad (6)$$

が成り立つ。

すでにみたように，$\tilde{f}(x)$ より小さい，f の FS 関数は存在しないから，$\tilde{f}(x)$ を情報無損失な FS 関数と呼ぶことにする。

つぎに，情報無損失な展開形式，すなわち，式(6) が等号

で成り立つようなF(x)のための展開形式が存在するかどうかについて考察する。

定義6. (5)式において，$i \neq j$ なる各i，jに対して，$x_i \cap x_j = \phi$ であるとき，(5)式を樹枝状展開という。

定理1. (5)式が樹枝状展開であるとき

$$\forall x \in \tilde{T}^n \quad \tilde{f}(x) = \tilde{F}(x) \tag{7}$$

がなり立つ．

証明. 樹枝状の仮定より

$$
\begin{aligned}
&\tilde{F}(x)\\
&= \tilde{F}(\tilde{f}_1(x_1), \cdots, \tilde{f}_r(x_r))\\
&= \{ F(b_1, \cdots, b_r) \mid b_1 \in \tilde{f}_1(x_1), \cdots, b_r \in \tilde{f}_r(x_r) \}\\
&= \{ F(b_1, \cdots, b_r) \mid b_1 \in \{f_1(a_1) \mid a_1 \leq x_1\}, \cdots, b_r \in \{f_r(a_r) \mid a_r \leq x_r\}\}\\
&= \{ F(f_1(a_1), \cdots, f_r(a_r)) \mid a_1 \leq x_1, \cdots, a_r \leq x_r \}\\
&= \{ f(a) \mid a \leq x \}\\
&= \tilde{f}(x)
\end{aligned}
$$

（証明終）

系．(5)式は二次の展開であるが，任意の次数の展開形式に対して，その中に用いられている関数すべてを"～"関数に変えて得られる関数値を$\tilde{F}(x)$で表すとき，この$\tilde{F}(x)$に

対して補題4および定理1がなりたつ。

与えられた関数$f(x)$がいつでも樹枝状展開をもつとは限らない。どんな$f(x)$に対しても，(6)式が等号で成立するような展開形式が存在するであろうか。$m=2$の場合については，主項展開がそれである.(2)．一般のm値の場合はいまのところ不明である。

4. 多値論理関数の多線式表現

本節では，非対称に誤る二値の入力および素子を用いて，多値論理関数のフェイルセイフシステムを構成する方法を提出する。

定義7. 以後，簡単のため三変数のm値論理関数$f(x, y, z)$を考える。（こうしても一般性を失わない）． 写像φ: $T \rightarrow \{0, 1\}^d$（d：自然数）のもとで，関数$\mathfrak{f}(\xi, \eta, \zeta)$が$f(x, y, z)$を二値表現するとは，ベクトル$\xi$, η, $\zeta \in \{0, 1\}^d$のd個の二値関数$f_0(\xi, \eta, \zeta), \cdots, f_{d-1}(\xi, \eta, \zeta)$が存在して，

$$\mathfrak{f}(\xi, \eta, \zeta) = (f_0(\xi, \eta, \zeta), \cdots, f_{d-1}(\xi, \eta, \zeta))$$

とかくとき，

$$\forall x, \forall y, \forall z \in T \quad \varphi(f(x, y, z)) = \mathfrak{f}(\varphi(x), \varphi(y), \varphi(z)) \qquad (8)$$

がなりたつときをいう。

このとき，多値論理関数 $f(x, y, z)$ は二値論理を用いて d 線式に表現されたという。明らかに，$d \geq [\log_2 m] + 1$ でなければならない。

$\boldsymbol{\xi} = (\xi_0, \cdots, \xi_{d-1})$ と表し，ξ_i を $\boldsymbol{\xi}$ の第 i 番目の要素という。第 i 番目の要素が 1 で他はすべて 0 であるような d 次元ベクトルを $\boldsymbol{\tau}_i$ で表す。

定義 8．写像 $\psi : T \to \{0, 1\}^m$ を $t_i \longmapsto \boldsymbol{\tau}_i$ で定義し，二値関数 $f_l(\boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta})$ $(l = 0, \cdots, m-1)$ を

$$f_l(\boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta}) = \sum_{i, j, k} a_{lijk}\, \xi_i \eta_j \zeta_k \qquad (9)$$

$$\begin{aligned} a_{lijk} &= 1 \ , \quad \text{if } f(t_i, t_j, t_k) = t_l \\ &= 0 \ , \quad \text{otherwise} \end{aligned}$$

（ここで加算と乗算はブール代数に従う）

で定義し，$\mathfrak{f}(\boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta}) = (f_0(\boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta}), \cdots, f_{m-1}(\boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta}))$ とかく。（$\boldsymbol{\tau}_i$ の定義は $d = m$ の場合で定義される），

定理 2．定義 8 で定義した関数 $\mathfrak{f}(\boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta})$ は写像 ψ のもと

でm値論理関数 $f(x, y, z)$ を二値表現する。

証明. $f(t_i, t_j, t_k) = t_l$ と仮定する。 このとき,

$\psi(f(t_i, t_j, t_k)) = \tau_l$ である. 一方

$$f_l(\tau_i, \tau_j, \tau_k) = a_{lijk} \cdot 1 \cdot 1 \cdot 1 = 1$$

また $h \neq l$ なる h に対しては $f_h(\tau_i, \tau_j, \tau_k) = 0$ となることは明らかであり, したがって, $\mathfrak{f}(\tau_i, \tau_j, \tau_k) = \tau_l$ となり, (8) 式が成り立つ。 (証明終)

定義 9. 写像 ψ を写像 $\tilde{\psi}: \tilde{T} \to \{0, 1\}^m$ へつぎのように拡張定義する。 $x \in \tilde{T}$, $\xi \in \{0, 1\}^m$ に対して,

$$\tilde{\psi}(x) = \xi \Leftrightarrow (t_i \in x \Leftrightarrow \xi_i = 1) \qquad (10)$$

また, ベクトル $\xi, \eta \in \{0, 1\}^m$ の和 $\xi + \eta$ を

$$[\xi + \eta]_i = \xi_i + \eta_i$$

で定義する。

補題 5. ベクトルの集合 $\{\xi^{(i)}\}$, $\{\eta^{(j)}\}$, $\{\zeta^{(k)}\}$ があるとき, 定義 8 で定義された関数 $\mathfrak{f}(\xi, \eta, \zeta)$ について,

$$\mathfrak{f}\left(\sum_i \boldsymbol{\xi}^{(i)},\ \sum_j \boldsymbol{\eta}^{(j)},\ \sum \boldsymbol{\zeta}^{(k)}\right) = \sum_i \sum_j \sum_k \mathfrak{f}(\boldsymbol{\xi}^{(i)},\ \boldsymbol{\eta}^{(j)},\ \boldsymbol{\zeta}^{(k)})$$

がなりたつ。

証明. ベクトル$\boldsymbol{\xi}$, $\boldsymbol{\xi}' \in \{0, 1\}^m$に対して

$$\mathfrak{f}(\boldsymbol{\xi}+\boldsymbol{\xi}',\ \boldsymbol{\eta},\ \boldsymbol{\zeta}) = \mathfrak{f}(\boldsymbol{\xi},\ \boldsymbol{\eta},\ \boldsymbol{\zeta}) + \mathfrak{f}(\boldsymbol{\xi}',\ \boldsymbol{\eta},\ \boldsymbol{\zeta})$$

を示せば十分である。いま, $[\boldsymbol{\xi}]_i = \xi_i$, $[\boldsymbol{\xi}']_i = \xi_i'$とする。任意の$l$に対して

$$f_l(\boldsymbol{\xi}+\boldsymbol{\xi}',\ \boldsymbol{\eta},\ \boldsymbol{\zeta}) = \sum_{i,j,k} a_{lijk}(\xi_i+\xi_i')\eta_j \zeta_k$$

$$= \sum_{i,j,k} a_{lijk}\xi_i \eta_j \zeta_k + \sum_{i,j,k} a_{lijk}\xi_i' \eta_j \zeta_k$$

がなりたつことより明らかである。（証明終）

定理3. (8)式で定義された関数$\mathfrak{f}(\boldsymbol{\xi}, \boldsymbol{\eta}, \boldsymbol{\zeta})$は写像$\tilde{\psi}$のもとで$m$値論理関数$f(x, y, z)$の情報無損失なFS関数$\hat{f}(x, y, z)$を二値表現する。

証明. $u \in \hat{T}$に対して

$$\tilde{\psi}(u) = \sum_{a \in u} \psi(a)$$

である。　ここに Σ はベクトルの加算である。　それ故，

$$\tilde{\psi}(\tilde{f}(x, y, z)) = \tilde{\psi}(\{f(a, b, c) \mid a \in x,\ b \in y,\ c \in z\})$$
$$= \sum_{a \in x} \sum_{b \in y} \sum_{c \in z} \psi(f(a, b, c))$$

一方，補題5より

$$\mathfrak{f}(\tilde{\psi}(x), \tilde{\psi}(y), \tilde{\psi}(z)) = \mathfrak{f}\left(\sum_{a \in x} \psi(a),\ \sum_{b \in y} \psi(b),\ \sum_{c \in z} \psi(c)\right)$$
$$= \sum_{a \in x} \sum_{b \in y} \sum_{c \in z} \mathfrak{f}(\psi(a), \psi(b), \psi(c))$$

ところが，定理2より

$$\psi(f(a, b, c)) = \mathfrak{f}(\psi(a), \psi(b), \psi(c))$$

であるから

$$\tilde{\psi}(\tilde{f}(x, y, z)) = \mathfrak{f}(\tilde{\psi}(x), \tilde{\psi}(y), \tilde{\psi}(z))$$

がいえる。　　　　　　　　　　　　　　　　　　　　　　（証明終）

以上の定理より，定義8による対応 ψ のもとで，$\psi(x) = \xi$，$\psi(y) = \eta$，$\psi(z) = \zeta$ と表わし，多値論理関数 $f(x, y, z)$ を

(9) 式で与えられる関数 $f(\xi, \eta, \zeta)$ で表わすことをフェイルセイフ表現ということにする。 なお，$|\xi| = \xi_0 + \cdots + \xi_{m-1}$ とすると，(9) 式は $|\xi|=1$，$|\eta|=1$，$|\zeta|=1$ なる関係式を用いて簡単化できる場合がある。

例 1. 次表で与えられる 3 値論理関数に対して，フェイルセイフ表現は

表 2.

x	1	1	1	2	2	2	3	3	3
y	1	2	3	1	2	3	1	2	3
$f(x,y)$	3	2	1	2	2	2	3	2	2

$$f_1(\xi, \eta) = \xi_1 \eta_3$$

$$f_2(\xi, \eta) = \xi_1 \eta_2 + \xi_2(\eta_1 + \eta_2 + \eta_3) + \xi_3 \eta_3$$

$$= \xi_1 \eta_2 + \xi_2 + \xi_3 \eta_3$$

$$f_3(\xi, \eta) = \xi_1 \eta_1 + \xi_3 \eta_1$$

で与えられる。

例 2. $T = \{t_0, \cdots, t_{m-1}\}$ が半順序 $\leq$ をもち，最小元を t_0，最大元を t_{m-1} とする束であるとする。 演算 $\wedge$，$\vee$ は

$$x \wedge y = \min\{x, y\} \tag{11}$$

$$x \vee y = \max\{x, y\} \tag{12}$$

で定義される。(5). これらの関数のフェイルセイフ表現を，(11) 式に対しては $f(\xi, \eta)$ ，(12) 式に対しては $g(\xi, \eta)$ とする。 $f_\ell(\xi, \eta)$，$g_\ell(\xi, \eta)$ はそれぞれ

$$f_\ell(\xi, \eta) = \xi_\ell \sum_{t_i \geq t_\ell} \eta_i + \eta_\ell \sum_{t_i \geq t_\ell} \xi_i$$

$$g_\ell(\xi, \eta) = \xi_\ell \sum_{t_i \leq t_\ell} \eta_i + \eta_\ell \sum_{t_i \leq t_\ell} \xi_i$$

であたえられる。 とくに

$$f_0 = \xi_0 + \eta_0, \quad f_{m-1} = \xi_{m-1}\eta_{m-1}$$

$$g_0 = \xi_0\eta_0, \quad g_{m-1} = \xi_{m-1} + \eta_{m-1}$$

である。 ここで，$m=2$ とおけば，二値の場合の，従来よく知られているフェイルセイフ表現が得られる。

5. 多値ユネイト関数

前節までは，フェイルセイフの条件として，情報の拡散の誤りのみを認めた。 本節では，出力値の集合の上にある半順序を仮定し，その半順序に従って大きい方への誤りが認められるものとしよう。

定義10.　m値論理関数 $f(x_1, \cdots, x_n)$ が与えられたとき，出力値の集合の上の半順序 $\leq_0$，入力値の集合の上の半順序を，変数 $x_1, \cdots, x_n$ に応じて $\leq_1, \cdots, \leq_n$ とし，$\leq_I$ を

$$\mathfrak{x} \leq_I \mathfrak{x}' \Leftrightarrow x_1 \leq_1 x_1', \cdots, x_n \leq_n x_n'$$

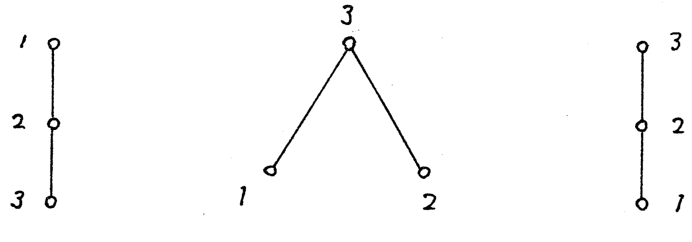
で定義する．$f(\mathfrak{x})$ が順序 $(\leq_I, \leq_0)$ に関して単調であるとは，

$$\forall \mathfrak{x}, \forall \mathfrak{x}' \in T^n \quad \mathfrak{x} \leq_I \mathfrak{x}' \Rightarrow f(\mathfrak{x}) \leq_0 f(\mathfrak{x}')$$

の成り立つときをいう。$\leq_0, \leq_1, \cdots, \leq_n$ がすべて恒等関係でないとき，$f(\mathfrak{x})$ はユネイトであるという。

例3．例1の関数 $f(x, y)$ について，各半順序が次の図のように与えられる。

図 1

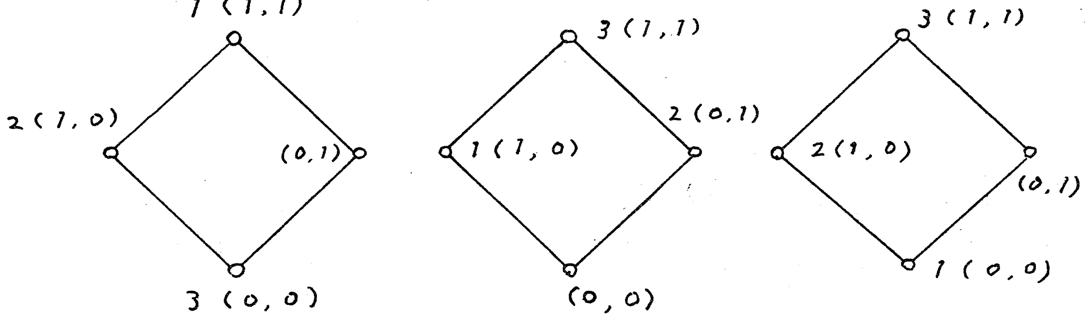


$\leq_0$　　$\leq_x$　　$\leq_y$

この節でのフェイルセイフの条件を少し変更して，半順序$\leq_0$に関して大→小の誤りを禁止することにする。上記の半順序を埋め込むようにコーディングすれば，本節でのフェイルセイフ条件をみたす二値フェイルセイフシステムを構成することができる。

例4. 例3の半順序は次の図のようにcodingできる。

図 2



本節の問題は稿を改めて詳細に論ずることにする。

おわりに，本題について，いろいろご討論して頂いた，京都大学の茨木俊秀氏，長谷川助教授，および三根教授に感謝する。

文 献

(1) 渡辺，高橋，"フェイルセイフ形論理系の一構成法"，昭40年信学全大

(2) 三根，高岡，"非対称故障論理回路を用いた2重系の一構成法，"信学会オートマトン研資（1967−09）.

(3) 平山，渡辺，浦野，"Fail-Safe 論理系の構成理論，"信学論（C），52−C，7，p.33（昭44−12）.

(4) 向殿政男，"C形 Fail Safe 論理の数学的構造について，"信学論（C），52−C，12，p812（昭44−12）.

(5) 伊藤誠，"n 値函数束（n 値論理に就て（I）），"九大工学集報，28，2（昭30）.