動的故障診断システムのモデル構成

池田　誠・藤本司郎

Dynamic Diagnosis Models

Makoto IKEDA and Jiro FUJIMOTO

Abstract

A graph-theoretic model for diagnosis is defined that each unit in its system can test the state each other and produce the unfault or fault syndrome in accordance with the result. Although a number of research concerning the diagnosis model (such as Preparata et al., 1976) has been discussed, any result has not come to be on a practical stage. The reason is that the probability of the fault occurence in each unit has been assumed to be constant or static in term t. Inferencely, it is possible to design a specified diagnosis model only in case that the dynamic system diagnosis can be applied.

On the assumption that the diagnosis models are dynamic in this paper, we can focus on testing self-diagnosable system including the dual directed testing and also on ploblem about system connection assignment. Moreover, the futher discussion will testify the higher reliability in the systems with these dianosis models.

1. まえがき

コンピュータシステムの適用範囲が広がるにつれて，そのシステムが正常に動作していることを保証する作業は重要でかつ複雑になってくる。システムの正常動作を保証すること，すなわち高信頼化手法には診断技術と冗長化技術の異なった2つの方法がある。従来こうした問題点に対して，故障の影響を冗長化技術により回避し，故障の存在は診断手続きにより検出している。

初期の故障診断は，熟練した保守技術者と特殊なハードウェアにより行なわれていた。この手法では，保守技術者の技能と詳細な知識とにほとんど依存していたので，システムが大きく複雑になるにつれてこのような方法では実際的ではなくなってきた。

そこで，C. V. Ramamoorthy は故障診断の問題にグラフ理論の適用を考察した。それはディジタルシステムの構成要素にグラフの節点 (node) を割り当て，グラフの線 (edge) を信号経路に対応させた。つぎに，この結果を使いシステムを組合せリンク (link) および最大の強連結サブグラフ (maximal strongly connected Subgraphs) の順序サブシステムに分割できるようにした。グラフの連結マトリクス (Connectivity Matrix) を操作するアルゴリズムは，マトリクスの乗算や分割化を必要とせず，大きなシステムの自動的分割を可能とした。

近年では，システムを構成しているユニットが故障しているときに，他の正常なユニットによりそれを検査できるシステムとして，自己診断可能なシステムの解析，構成問題等について議論されている[1)-7)]。Preparata ら[1)]はシステムを複数個の部分システムに分割し，各部分システムをユニットとしたときに，最高 t 個の故障が同時にシステム内に存在しても検査結果（以下シンドロームと呼ぶ）からすべての故障ユニットを検出することのできる t 重故障同時診断可能 (t-fault one-etep diagnosable) なシステムと，少なくともひとつの故障ユニットを検出することのできる t 重故障逐次診断可能 (t-fault sequentially diagnosable) なシステムについて診断可能なシステムが存在する為の必要十分条件，診断可能な最適システムの構成問題などの研究がなされた。Russell ら[2),3)]は，枝と検査が一対一に対応しているこの診断モデルを多対一対応に拡張したシステムを提案した。また，Maeshwari ら[4)]は各構成ユニットに固定的な故障確率を導入した確率的診断モデルを提案し，t 重故障同時診断可能システムであるための必要十分条件を与えた。

Preparata らの診断可能システムでは，システムを構

昭和57年10月12日受理

成しているユニットがすべて等しい故障確率であるという仮定のもとでシステムの存在定理等について議論している。又，Maheshwari らによるシステムでは同様に一定故障生起確率に基づいて議論されている。ここでのユニットの故障生起確率は時刻Tに関して静的な状態でしか考察されていない。

上記のごとく Preparate らのシステムは実際のシステムに適用するモデルとしては不十分である。そこで筆者らはシステムモデルに動的な故障生起確率を持つシステムをモデルにして，故障生起確率が急激に変化するユニットを有する診断システムに，双方向検査の概念を導入し，新たにそのシステムの存在定理，最適システム構成方法を与える必要十分条件を提案した。

2. 定義と仮定

2.1 診断システムのモデル化

任意に与えられたシステムの各ユニットを節点とし，ふたつのユニット間の検査を有向枝に対応させることにより得られる有向グラフで診断を行なうことのできるシステムを自己診断可能なシステムと呼ぶ。

診断モデルの各々のユニットをグラフにおけるひとつの節点としたときに，節点の集合 $V=\{u\}$ と節点間に存在する弧 (u_i, u_j) $(i, j=1, 2, 3, \cdots, n)$ の集合 $E=(u_i, u_j)\}$ とで定まる有向グラフを $G=(V, E)$ で表現する。ユニット u_i がユニット u_j を検査したときのユニット間の結合状態を表わす集合の要素を b_{ij} とする。又，b_{ij} の重みとして $\rho(u_i, u_j)=(0, 1)$ を付加する。$\rho(u_i, u_j)=0$ は，ユニット u_i がユニット u_j を正常と評価したときとする。又，$\rho(u_i, u_j)=1$ は，故障と評価したときの状態を表わす。

［定義 1］ 検査のときの結合 $b_{ij}(i, j=1, 2, \cdots, n)$ の集合をシステムの結合と呼ぶ。このときの結合マトリクスは $C=\|C_{ij}\|$ で次のように決める。

$$C_{ij}=\begin{cases} 1 \cdots b_{ij} \text{ が存在する} \\ 0 \cdots b_{ij} \text{ が存在しない。} \end{cases}$$

［定義 2］ テスト結果 $\rho(u_i, u_j)$ の集合をシステムのシンドロームと呼ぶ。シンドロームは b_{ij} が存在しているときのみ割り当てられる。

次に実際の例で故障ユニットを検査する方法を考察する。

［例 1］ 5つのユニット $u_1, u_2, \cdots, u_5$ から構成されるシステムを考えた場合，ユニット間の結合が図2-1のように $b_{12}, b_{23}, b_{45}, b_{51}, b_{13}, b_{35}, b_{52}, b_{24}, b_{41}$ であったとする。このシステムの結合マトリクス C は

$$C=\begin{pmatrix} 0&1&1&0&0 \\ 0&0&1&1&0 \\ 0&0&0&1&1 \\ 1&0&0&0&1 \\ 1&1&0&0&0 \end{pmatrix}$$

となる。又，このシステムのシンドローム E は，

$$E_1=[\rho(u_1, u_2),\ \rho(u_2, u_3),\ \rho(u_3, u_4),\ \rho(u_4, u_5),\ \rho(u_5, u_1)]$$

$$E_2=[\rho(u_1, u_3),\ \rho(u_3, u_5),\ \rho(u_5, u_2),\ \rho(u_2, u_4),\ \rho(u_4, u_1)]$$

で表現できる。今このシステムの u_1 と u_5 が故障ユニットであった場合のシンドロームは，

$$E_1=(x,\ 0,\ 0,\ 1,\ x)$$

$$E_2=(x,\ 1,\ x,\ 0,\ 1)$$

となる（但し，x は故障ユニットが他を検査したときで，0か1のあいまいな結果となることから x としている）。図2-2(a) はシンドローム E_1 に対する部分システムである。同様に (b) は E_2 に対する部分システムである。

このようにして与えられた任意のシンドローム E より故障ユニットを認証することは容易である。それは，任意のシンドローム又はその循環順列に連続な数値 001

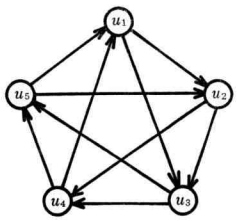

Fig. 2–1. A system consisting of five units.

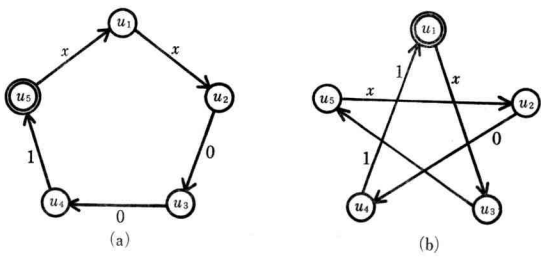

Fig. 2-2 Two different faulty condition exhibiting the same syndrome. Faulty units are doneted with double circles.

が存在するとき，その数値で1である部分が故障ユニットの検査となる。又，001 が存在しないときは 1101 が与えられる。この検査結果からは連続な数値で最後の1が故障ユニットの検査となる。従って，E_1 からはユニット u_5 が，E_2 からはユニット u_1 が各々故障していることがわかる。このようにして，あるシステムに存在する故障ユニットを任意のシンドローム E により検査するシステムを総称して自己診断可能なシステムという。

［例　終］

次に t 重同時故障診断可能と t 重確率的故障診断可能なシステムについて，それらの存在定理と最適システム構成について議論する。

2.2　t 重同時故障診断可能システム

システム S の診断モデルを $S=(V, \Gamma)$ で表現する。但し，

V はユニットの集合

Γ: $V \to 2^V$ は接続関数でユニット u_i がユニット u_j を検査したときに，$u_j \in \Gamma(u_i)$ とする。Γ が定義されていないシステムを $S=(V, -)$ で表わす。

このシステム $S=(V, \Gamma)$ は明らかに有向グラフ $G=(V, \Gamma)$ によって表現できる。又，任意のシンドロームに対して与えられる故障ユニットの集合を次のように定義する。

［定義　3］ 次の条件 1，2 を満たす V の部分集合 F をシンドロームに関する無矛盾故障集合とする。

(条件　1)　$u_j \in \Gamma(u_i)$，$u_i \in F = V-F$，$u_i \in F$ なるすべての u_i，u_j に対して $\rho(u_i, u_j)=1$。

(条件　2)　$u_j \in \Gamma(u_i)$，$u_j \in F$ なるすべての u_i，u_j に対して $\rho(u_i, u_j)=0$.

［定義　4］ 任意のシンドロームにおいて，t 個のユニットからなる無矛盾故障集合がたかだかひとつしか存在しないで，かつすべての故障状態にあるユニットを検査できるシステムを t 重同時故障診断可能システムという。

次にシステムを構成するユニット群が与えられたとき，診断可能なシステムを構成できるかどうかの判定問題，すなわちシステム $S(V, -)$ が与えられたときに，$\hat{S}=(V, \Gamma)$ が診断可能となるような Γ が存在するための必要十分条件を示す。

［定理　1］ 任意のシステム $S=(V, -)$ が与えられたとき，$\hat{S}=(V, \Gamma)$ が t 重同時故障診断可能となるような関数 Γ が存在するための必要十分条件は，故障ユニットの個数 t が $t \geq (n-1)/2$ であることである（但し，n はユニット総数）

(証明)　$\hat{S}=(V, \Gamma)$ の Γ として，

$u \in V$ に対して，$\Gamma^{-1}(u)=\{u\}$

$u \notin V$ に対して，$\Gamma^{-1}(u)=V-\{u\}$

と定義する。明らかに Γ は接続条件を満たしている。V の中に正常なユニットが少なくとも一つあれば，明らかにすべてのユニットの状態を識別でき，無矛盾故障集合が一意的に判定される。

ここで，すべて完全に検査された z 個からなるユニットの部分集合が存在するとしよう。もし，$z \geq t+1$ ならば，すべての検査は正常で，これは故障が許される最大ユニット数を表わす。この $t+1$ 個の無矛盾故障集合が直接故障集合，すなわち n 個のユニットで構成されたシステムに接続され検査される。従って，t 個の故障が存在する S は，少なくとも $t+1$ 個の正常ユニットがなければ正常に診断することができない。

(必要条件)　システム S が，$n<2t+1$ 個のユニットで構成されていると仮定する。ここで $n=2t_0$ $(t_0 \leq t)$ となるような t_0 を設け，システム S を P_1，P_2 に分割する。P_1 のユニットはすべて故障，P_2 はすべて正常と仮定する。部分システム P_2 の中で行なわれる検査に関してはすべて0となり，P_2 から P_1 への検査はすべてと1なる。これに対して，部分システム P_1 では，ユニットがすべて故障しているので，その内部での値は0か1のあいまいな値となる。この場合に，P_1 内部での検査がすべて0となってしまった場合，P_1 から P_2 の検査は1となってしまう，従ってこのようなシステムは t 重同時故障診断可能なシステムとはならない，　(証明終)

最適システムの構成問題でのひとつの解は診断グラフでの検査数 $(\sum_{u \in v} |\Gamma(u)|)$ が最小であるシステムと定義できる。

［定理　2］ t 重同時故障診断可能システムでは，一つのユニットが他の t 個のユニットにより検査される。

(証明)　システム S を t 重同時故障診断可能システムとし，$u_1, u_2, \cdots, u_k$ をシステム S のユニットとし，u_0 を正常なユニット，$k<t$ と仮定する。ユニット $u_1, \cdots, u_k$ がすべて故障していたとすると，これらの故障ユニットから検査した結果はすべてあいまいなものとなる。このことから，この検査は信頼のおけるものとは言えず，シンドロームは $(u_1, u_2 \cdots, u_k)$ と $(u_0, u_1, \cdots, u_k)$ となり，故障ユニットが t 個以上存在するシステムでは故障を識別できない。従ってシステム S は定義1より，t 重同時診断可能とは言えない。　(証明終)

定理1と定理2より，t 重同時故障診断可能システム

の最適システムは，システムを構成するユニットの総数を n とすると，次のようになる。

［定義 5］ 任意のシステム S が最適な t 重同時診断可能なシステムとなるには，$n=2t+1$ 個のユニットから構成され，かつ t 個の他のユニットによって検査されたようなシステムとなる。

ひとつの最適解として，Preparate らは $D_{\delta t}$ システムを提案している。$D_{\delta t}$ システムとは，ユニット u_1, u_2, $\cdots$ u_n からなり，$j-i=\delta_m$ (modulo n)，$1\leq m\leq t$ のときに限り，ユニット u_i からユニット u_j へ枝があるシステムで，$(\delta, n)=1$ (δ と n は互いに素) である場合に，t 重同時故障診断可能システムの最適解となる。このようにして考えたシステム $D_{\delta t}$ を図2-3に示す図2-3(a) は D_{12} システムで，(b) は D_{22} システムである。

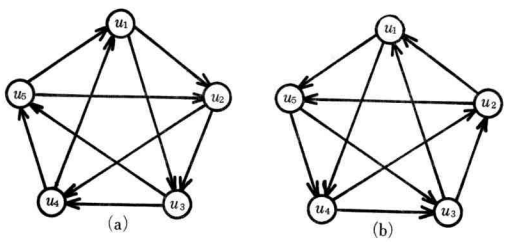

Fig. 2–3. Two designs for one-step t-fault diagnosis.

2.3 t 確率的診断可能システム

2.2のシステムでは，すべてのユニットの信頼性を同等と仮定していたが，より現実的な議論を行なうために故障生起確率に基づき診断能力の尺度 t を導入した場合の診断可能システムについて，その存在定理とシステム構成に関する問題について考察する。

システム S の診断モデルを $S=(V, \Gamma, p)$ で表現する。但し，p: $V\to R$ は各ユニットの故障確率で，R は0から1までの実数値とする。これは2.2と同様に診断モデル $S=(V, \Gamma, p)$ が有向グラフ $G=(V, \Gamma)$ によって表現できる。

対象となるユニットの故障が互いに独立であるとすると，任意の部分集合 $F\subset V$ が故障集合である確率 $P(F)$ は

$$P(F)=\prod_{u\in F}(1-p(u_i))\cdot\prod_{u\in F}p(u_i) \tag{1}$$

となる。

［定義 6］ 任意のシンドロームにおいて，$P(F)>t$ となる無矛盾故障集合 F がたかだか ひとつしか存在しないとき，システム $S=(V, \Gamma, p)$ は t 確率的診断可能であるという。

(1)式より，

$$\log P(F)=\sum_{u_i\in F}\log(1-p(u_i))+\sum_{u_i\ni F}\log p(u_i) \tag{2}$$

ここで，$P(F)>t$ とすると(2)式は，

$$\sum_{u_i\ni F}\log\left[\frac{1-p(u_i)}{p(u_i)}\right]<k(t) \tag{3}$$

$$k(t)=-\log t+\sum_{u_i\in V}\log(1-p(u_i)) \tag{4}$$

となる。又，

$$W(u_i)=\log\left[\frac{1-p(u_i)}{p(u_i)}\right] \tag{5}$$

とすると，$W(u_i)$ は各ユニットにおける故障確率の重み関数となり，これはシステム中の故障ユニットを検出するときに，無矛盾故障集合を決定するためのものである。すなわち，任意の故障集合 $F\subset V$ に対して，$P(F)>t$ は $W(F)<k(t)$ であることがわかる (但し，$W(F)=\sum_{u_i\in F}W(u_i)$)。従って t 確率的診断可能なシステムにおいて故障ユニットを検出する問題は，それに属する節点の重みの和が $k(t)$ より小さい無矛盾故障集合を求める問題と等しい。従って診断システム $S=(V, \Gamma, p)$ の表現と同様に，$S=(V, \Gamma, W)$ の表現も可能となる。

関数 Γ の定義域及び値域を拡張すると以下のようになる。

$$\Gamma(u_i)^{-1}=\{u_j/u_i\in\Gamma(u_j)\}$$

$X\subset V$ に対して

$$\Gamma(x)=\{\bigcup_{u_i\in X}\Gamma(u_i)\}-X$$

$$\Gamma^{-1}(x)=\{\bigcup_{u_i\in X}\Gamma^{-1}(u_i)\}-X$$

システム $S=(V, \Gamma, W)$ が t 確率的診断可能となる必要条件は次の補題で示される。

［補題 1］[4] 有向グラフ $G=(V, \Gamma)$ で与えられたシステム S があったとき，$W(u_i)+W(\Gamma^{-1}(u_i))\geq k(t)$ であれば t 確率的診断可能なシステムである。

補題1よりシステムの存在定理は次のようになる。

［定理 3］[4] 任意のシステム $S=(V, -, W)$ が与えられたとき，$\hat{S}=(V, \Gamma, W)$ となる関数 Γ が存在するための必要十分条件は，V の任意の分割 $\{U_1, U_2\}$ に対して，共に $W(U_1)<k(t)$，$W(U_2)<k(t)$ とはならないことである。 (証明略)

この定理3は明らかにすべてのユニットにおける故障確率が等しい場合，故障ユニットの個数が $t\geq(n-1)/2$ となることから，定理1が拡張されているということがわかる。

次に t 確率的診断可能なシステムの構成について考察する。

［定義　7］ 任意のシステム S に対して，一般性を失なうことなく各々の故障ユニットの重みが，$W(u_1) \leq W(u_2) \leq \cdots W(u_n)$ であると仮定する。各 $u_i \in V$ に対してある β が存在するとして，

$$\Gamma(u_i) = \left\{ u_{i+1}, u_{i+2}, \cdots, u_\beta \middle| \sum_{j=i+1}^{\beta} W(u_j) < k(t) \sum_{j=i+1}^{\beta+1} W(u_j) \geq k(t) \right\}$$

（但し，$\Gamma^{-1}(u_i) = \phi$）

となるとき，システム $S=(V, \Gamma, W)$ を $D_{\delta t}^{\phi}$ システムという。

［定理　4］ 定理3の条件を満たす $D_{\delta t}^{\phi}$ システムは，定義6のシステム全体に属する。

（証明）　故障確率の大きさの順に並べたユニットの系列 $\bar{V} = u_1, u_2, \cdots, u_n$ に注目する。今系列 V の中で連続して故障状態であるユニット群をまとめて $\bar{f}_i$ で表し，故障ユニット群と故障ユニット群の間の正常状態のユニット群も同様にまとめて $\bar{g}_i$ で表わすとすると，V は $\bar{V} = \bar{g}_0 \bar{f}_1 \bar{g}_1 \cdots \bar{f}_l \bar{g}_l$，$\bar{g}_0$，$\bar{g}_l$ は空であっても構わないが，$\bar{g}_i (1 \leq i \leq l-1)$ は空ではない。系列 X を構成するユニットの集合を X で表し，集合 f_i に属するユニットの添字を適当に書換え，$f_i = \{u_{i1}, u_{i2}, \cdots, u_{in(i)}\}$ と表し，$|f_i| = n(i)$ とする。このような表現形式を採用すると，無矛盾故障集合 F は $F = f_1 U f_2 U \cdots U f_l$，$W(F) = \sum_{j=1}^{l} W(f_j) < k(t)$ と書ける。すべての f_i において，

$$\sum_{j=1}^{n(i)} W(i,j) < k(t) \quad \text{且つ} \quad \sum_{j=1}^{n(i)+1} W(u_{i,j}) < k(t)$$

である場合，すべての f_i に対して，$u_{iu(i)+1} \in \Gamma(u_{io})$ が言える。但し，$i_0 = i_1 - 1$ とする。システムの診断グラフ $G=(V, \Gamma)$ において有向枝 $(u_{io}, u_{in(i)+1})$ が存在し u_{io}，$u_{in(i)+1}$ は共に正常であるから，そのシンドロームは，$\rho(u_{io}, u_{in(i)+1}) = 0$ である。従ってこの場合，系列 $U = \tilde{g}_0 \tilde{g}_1 \cdots \tilde{g}_l$ は有向閉路をなし，この有向閉路上のシンドロームの値がすべて "0" であることがわかる。しかも定理3の条件を満たすから，$W(U) = W(V-F) \geq k(t)$ となる。従って，U に属するユニットはすべて正常であることがわかる。U に属するユニットから残りのユニットの故障状態を識別することができる。（証明終）

このようにして構成された $D_{\delta t}^{\phi}$ システムでは，すべてのユニットが等しい故障確率を持つ場合に，2.2 の T 重同時故障診断可能システム $LD_{\delta t}$ と一致する。但し，この場合の T は次の不等式を満たす最大整数とする。

$$T < \left\{ \frac{k(t)}{\log[(1-p)/p]} \right\} \tag{6}$$

次に定義7より構成されるシステムの例を示す。

［例　2］ 5個のユニット u_1，u_2，$\cdots$，u_5 からなるシステム $S=(V, \Gamma, W)$ について，$D_{\delta t}^{\phi}$ システムを作る。各ユニットの故障確率として，$p(u_1) = 1/3$，$p(u_2) = p(u_3) = 1/4$，$p(u_4) = 1/5$，$p(u_5) = 1/6$ とすると，$W(u_i)$ は(5)式より各々 $W(u_1) = \log 2$，$W(u_2) = W(u_3) = \log 3$，$W(u_4) = \log 4$，$W(u_5) = \log 5$ となる。又，$k(t) = \log 8$ とする。このとき $W(V) = \sum_{i=1}^{5} W(u_i) > 2k(t)$ となり，システム S の Γ は定理3の存在定理を満足する。定義7より各々の接続関数 Γ は $\Gamma(u_1) = \{u_2\}$，$\Gamma(u_2) = \{u_3\}$，$\Gamma(u_3) = \{u_4\}$，$\Gamma(u_4) = \{u_5\}$，$\Gamma(u_5) = \{u_1, u_2\}$ となる。従って $\hat{S}$ の診断グラフ $G=(V, \Gamma)$ は図2-4(a)となる。$\hat{S}$ の検査数 R は，$R = \sum_{i=1}^{5} |\Gamma(u_i)| = 6$ である。比較のため，すべてのユニットが $p=1/3$ となる故障確率を有するときのシステムを(b)に示す。このときの T は(6)式より2であり，図2-3と一致することがわかる。〔例終〕

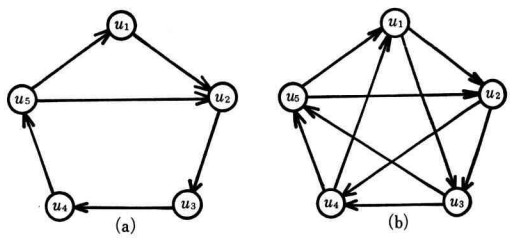

Fig. 2-4. Design $D_{\delta t}^{\phi}$ for a system with five units

3. 既存モデルの問題点
—dynamic 診断システムの必要性—

Preparata ら[1] のシステムでは，議論を簡単にするためにすべてのユニットの信頼性（故障確率）を同等に考えている。また，各ユニットの故障確率を考慮して議論された Maheshwaria らのシステムは，Preparata らのシステムはらのシステムの拡張モデルとして与えられていることを認識できる。しかし，それらのシステムでは単に故障確率を固定的（静的）にしか把握していない。ところが，通常存在しているシステムにおける部分システム（各ユニット）の故障確率は，必ずしも静的であるとは限らない。換言すれば，故障生起確率は時刻 t によって変化することを考えなければならない。

ある標準的な装置（システム）について，例えば，それがハードウェアであった場合の瞬時故障率の時間的変化を図3-1に示す。初めのうちは，このシステムS1の方が故障率を早い時期に発見することで信頼性は最高点に達する。この初期の時間が過ぎると，比較的一定した故障頻度に落着く。このシステムが通常の耐用年数の終わりに近づくと故障頻度は増す。また，システム $S2$ では，初めのうち故障率はシステムS1より低いが，比較的一定した故障頻度に落着くときに，S1より高い故障率で一定し，耐用年数も短い。

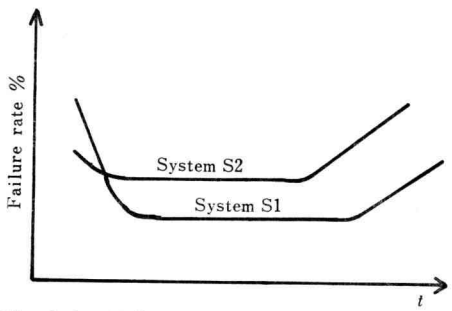

Fig. 3–1, Failure rate for system S1 and S2.

このように時刻 t の変化により故障率の異なるシステムS1, $S2$ を部分システムとするような診断可能モデルを設計する場合，今まで述べてきた診断モデルであることは明白である。極めて一般的な故障状態（時刻 t によって各々のユニットの故障確率が変化するような状態）にシステムがあるとき，故障確率が時刻 t により変化するような動的 (dynamic) システムが必要となる。実際のシステムモデルにおいて，故障確率が動的であった場合の問題点を例3に示す。

［例 3］ 5個のユニット $u_1, u_2, \cdots u_5$ からなる確率的診断可能システム $\hat{S}_1$ が与えられ，各々のユニットの故障確率が時刻 t において，$p(u_1)=1/3$, $p(u_2)=1/4$, $p(u_3)=p(u_4)=1/5$, $p(u_4)=1/6$ であったとする。また $k(t)=\log 8$ であったとき，時刻 t におけるシステム $\hat{S}$, の Γ は定義7参照）より求めることができる。こうして構成されたシステム D^{ϕ}_{st} を図3-2(a)に示す。次に任意の時刻 t^* において，各々のユニットの故障確率が，$p(u^*)=p(u_2^*)=1/4$, $p(u_3^*)=1/3$, $p(u_4^*)=1/6$, $p(u_5^*)=1/3$ と各々変化したときを考える。定義7の仮定により，各々のユニットは，$u_3^* \to u_1^{**}$, $u_5^* \to u_2^{**}$, $u_1^* \to u_3^{**}$, $u_2 \to u_4^{**}$, $u_4^* \to u_5^{**}$ に対応しているとき，$D^{\phi^*}_{st}$ システムは図3-2(b)となる。

このように構成されたふたつのシステムは，時刻 t から時刻 t^* までの間，同時に存在すると考えられる。また，各ユニットの故障確率は ρ から ρ^* に変化はしているが，ユニットそのものは変わっていないと考えるのが普通である。このような考えの下で $D_{st}{}^{\phi}$ システムと $D_{st}{}^{\phi^*}$ システムが同時に存在する場合の有向グラフ $G=(V, \Gamma)$ を図3-2(c)に示す。（実線は $D_{st}{}^{\phi}$ システムの，点線は $D_{st}{}^{\phi^*}$ システムの検査を表わす。）

図3-2(c)に注目すると，同方向に並列な検査［$u_2 \in \Gamma(u_1)$, $u_5 \in \Gamma(u_4)$ 及び $u_1 \in \Gamma(u_5)$］と逆方向に並列な検査［$u_4 \in \Gamma(u_3)$, $u_3 \in \Gamma(u_4)$］が存在していることがわかる。同方向に並列な検査は単に冗長検査としてシステムから除去できる。しかし，動的システムを設計するときに，逆方向に並列な検査（以下，双方向検査とする）が必要となってくる。 ［例 終］

以上のことにより，動的システムを構成するためのシステム構成法のひとつとして，双方向検査を有する診断システムの存在定理とシステムの構成問題を議論する。

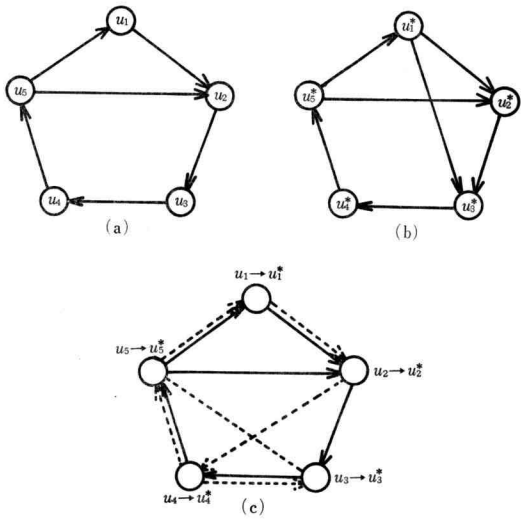

Fig. 3–2. Design $D_{\delta t}{}^{\phi}$ for a system with time t.

4. 双方向検査を有する診断可能システム

4-1 診断モデルと診断可能性

システムの診断モデルを $S=(V, V_1, \Gamma)$ で表わす。ここで，V_1 は検査されたユニットが検査したユニットを検査できる（以下，双方向検査とする）ユニットの集合とする。

$X \subseteq V$ に対して，

$$\Gamma(X) = \bigcup_{u \in X} \Gamma(u)$$

$$\Gamma^{-1}(X) = \bigcup_{u \in} \Gamma^{-1}(u)$$

と定義する。明らかにこの診断モデルはグラフ $G=(V, \Gamma)$ によって表現できる。

双方向検査可能なユニットを導入したとき，接続関数 Γ は次の条件を満たす必要がある。

［接続条件］

(1) $u_i, u_j \in V_1 = V - V$ に対して，$u_j \in \Gamma(u_i)$ なら $u_j \in \Gamma^{-1}(u_i)$

(2) $u_i \in V_1, u_j \in V_1$ に対して，$u_j \in \Gamma(u_i)$ なら $u_j \in \Gamma^{-1}(u_i)$.

次に 2·2 の定義 3 に加え，双方向検査を含む任意のシステムにおける故障ユニットの集合を示す。

［定義 8］ 2·2 の条件 1.2 及び次の条件 3, 4 を満たす V の部分集合 F をシンドローム ρ に関する強無矛盾故障集合とする。

(条件 3) $u_j \in \Gamma(u_i)$, $u_i \in \Gamma(u_j)$, $u_i, u_j \in F = V - F$ なるすべての u_i, u_j に対して，

$$\rho(u_i, u_j) = 0, \quad \rho(u_j, u_i) = 0.$$

(条件 4) $u_j \in \Gamma(u_i)$, $u_i \in \Gamma(u_j)$, $u_i \in F$, $u_j \in F$ なるすべての u_i, u_j に対して，

$$\rho(u_i, u_j) = 1, \quad \rho(u_j, u_j) = x.$$

定義 8 の強無矛盾故障集合に関して，t 重同時故障診断可能となるシステムを定義 4 と同様に次のように決める。

［定義 9］ 任意のシンドローム ρ に対して，たかだか t 個のユニットからなる強無矛盾故障集合がたかだかひとつしかないとき，このシステム t を重同時故障診断可能なシステムいう。

4·2 診断可能システムの存在定理

システムを構成するユニット群が与えられたとき，各々のユニットが持つ検査機能が故障診断の可能なシステムを構成できるかについて議論する。

［定理 4］ 任意のシステム $S=(V, V_1, -)$ が与えられたとき，$S=(V, V_1, \Gamma)$ が t 重同時故障診断可能となるような接続関数が存在するための必要十分条件は，$|V| > |V_1|$ の場合，故障ユニットの個数 t が $t \geq (n-1)/2$ で，$|V| = |V_1|$ のとき $t \geq n-1$ となることである。(但し，n はユニットの総数)

(証明) $\hat{S}=(V, V_1, \Gamma)$ の Γ として，

$u_i \in V_1$, $u_j \in \bar{V}_1$ に対して，$\Gamma^{-1}(u_j) = \{u_j\}$,

また $\Gamma^{-1}(u_i) = \{u_j\}$

とすれば，関数 Γ は明らかに接続条件を満たす。今 u_i, u_j に注目すると，これらふたつのユニットは対称律を満たしていることがわかる。Preparata ら[1] の定理 1 より，対称律を含まない診断グラフでは，故障ユニットの個数 t が $t \geq (n-1)/2$ であることが知られている。対称律を含むシステムを考えたとき。$u_i \in V_1$ のユニットに対して，$u \in \Gamma^{-1}(u_i)$ となるような検査数は増すことがわかる。しかし，$|V| - |V_1|$ 個のユニットに関しては，検査数が増えることがないので，故障ユニットの個数 t は $t\,2(n-1)/2$ となる。

$|V| = |V_1|$ となった場合，すべての $u \in V$ が $u \in V_1$ と同値になるので，これらのすべてのユニット u が対称律を満たすことになる。これは，各ユニットを検査するユニットの数が $2t$ 個となることに他ならない。従って故障ユニットの個数 t は $t \geq (n-1)$ となる。

(証明終)

$S=(V, V_1, \Gamma)$ の任意の $u_i \in V_1$, $u_j \in V$, に対して，$u_j \in \Gamma(u_i)$ となるシステム $S_*=(V, V_1, \Gamma_*)$ とすると，この S_* について次のことがいえる。

［定理 5］ S が t 重同時故障診断可能ならば，S_* も t 重同時故障診断可能である。

(証明) S_* が t 重同時故障診断可能でないシステムとすると，S_* における任意のシンドローム ρ_* に対して，$|F_1| \leq t$, $|F_2| \leq t$ なる $F_1 \neq F_2 \subseteq V$ が存在して，これらは ρ_* に関して無矛盾故障集合となる。

ρ_* よりシステム S のシンドローム ρ を作ると，

$u_j \in \Gamma(u_i)$, $u_i \in V$, $u_j \notin V_1$ に対して

$\rho(u_i, u_j) = \rho_*(u_i, u_j)$

$u_j \in \Gamma(u_i)$, $u_i \in V$, $u_j \in V_1$ に対して

$\rho(u_i, u_j) = \rho_*(u_j, u_i)$

となる。このようにして決めたシンドローム ρ に対してもやはり F_1, F_2 は無矛盾故障集合となるので，S は t 重同時故障診断可能ではない。　(証明終)

4·3 システム構成法

Preparata らの最適システム $D_{\delta t}$（定義 5 参照）から，双方向検査を含むシステム $D_{\delta t}{}^*$ を作成する。

(1) $u \in V$ なるすべてのユニット u に対して，定義 5 に従って $D_{\delta t}$ システムを作る。この診断グラフを $G_0=(V, \Gamma)$ とする。

(2) G_0 から次のような診断グラフ $G=(V, \Gamma)$ を作る。$u^* \in V_1$ に対して，$\Gamma(u^*) = u$.

以上の操作で作られたシステム $S=(V, V_1, \Gamma)$ を $D_{\delta t}{}^*$ システムと呼ぶ。$D_{\delta t}{}^*$ システムは t 重同時故障診断可能なシステムであることが，定理 5 よりわかる。図 4-1

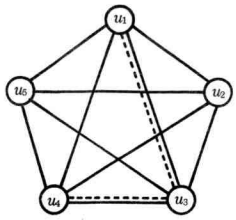

Fig. 4–1. Design D_{22}* for a system with five units.

に D_{22}* システムの例を示す。但し，$V_1=\{u_3\}$ とする。

双方向検査を含むシステム $D_{\delta t}$* での総検査数は，$(|V|+|V_1|)*t$ であることが定理4よりわかる。検査数に関してその数が最適システムの構成問題となるならばこのシステムは最適ではないが，動的診断システムを考えたときにはこの最適性（検査数の多い少ないという問題）は意味のないことになることが，4. の例題よりわかる。

む す び

本論文では自己診断システムの構成ユニットが動的な故障生起確率を有するときのシステムについて考察し，さらに双方向検査を含むシステムについて，t 重同時診断可能なシステムの必要十分条件と最小の検査数となるための最適システム構成方法を与えた。

システムを構成するユニットが動的な故障生起確率を有している場合，そのシステムに双方向検査方法を適用することは有効な手法であることが明確にされた。同時に考察されていなかった動的故障生起率を有する t 重同時診断可能なシステムの構成法を提案した。これは本論文の対象とした Preparata らの自己診断システムやそのシステムをさらに一般化した Russell と Kim の自己診断システムにおいて自己診断システムに双方向検査を導入することにより，その診断能力の信頼性を向上させた。この方法は，診断機能そのものに冗長度を増してより信頼性の高い検査が可能となるばかりでなく，動的に変化するユニットの故障生起確率を有するシステムの双方向検査導入を考慮している点で，より有効な高信頼性動的自己診断可能なシステムモデルであることが明確化された。

参 考 文 献

1) Preparata, F.P., Metze, G. and Chien, R.T.: "On the connection assignment problem of diagnosable systems", IEEE Trans. Electron. Comput., EC–16, p. 848 (eDc. 1967)
2) Russell, J.D. and Kim, C.R.: "System fault diagnosis: Closure and diagnosability with repair", IEEE Trans. Comput. C–24 p. 1078 (Nov. 1975)
3) Russell, J.D. and Kim, C.R.: "System fault diagnosis: Making exposure and diagnosability without repair", IEEE Trans. Comput. C–24, p. 1155 (DEC. 1975)
4) Maheshwari, S.N. and Hakimi, S.L.: "On models for diagnosable systems and probabilistic fault diagnosis", IEEE Trans. Comput. C–25, p. 228 (March 1976)
5) Allan, F.J., Kameda, T. and Toida, S.: "An approach to the diagnosability analysis of a system", IEEE Trans. Comput., C–25, p. 1040 (Oct. 1975)
6) Barsi, F., Grandoni, F. and Maestrini, P.: "A theory of diagnosability of digital systems", IEEE. Trans. Comput., C–25 p. 505 (June 1976)
7) Kameda, T. Toida, S. and Allan, F.J.: "A diagnosing algorithm for netwarks": Information and Control **29**, 141–148 (1975)