3B-5

断続的な故障を考慮したマルチプロセッサシステムのシステムレベル故障診断に関する研究

System-Level Diagnosis for Multiprocessor Systems in the Presence of Intermittent Faults

桐 大輔 † 山田 敏規 †
Daisuke Kiri Toshinori Yamada

1. はじめに

マルチプロセッサシステムのシステムレベル故障診断のためのグラフ理論的な枠組みは Preparata ら [3] によって提案され，この枠組みは PMC モデルとして広く知られており, PMC モデルに基づいたマルチプロセッサシステムの故障診断に関する研究がこれまでに数多く行われている．PMC モデルでは, 各プロセッサは正常もしくは (常時) 故障のどちらか一方の状態をとり, 故障診断の最中にこの状態が変わることはないと仮定する．また, システム内の故障プロセッサの数は制限されていると仮定する．各プロセッサは通信リンクを介して隣接するプロセッサの検査を行い，もし正常であると判断したならば 0 を, 故障していると判断したならば 1 を出力する．但し, 正常なプロセッサが行う検査結果は常に正しいが, 故障しているプロセッサの検査は全く信頼できないものとする．マルチプロセッサシステム内で行われるプロセッサ同士の検査は, プロセッサを点で, プロセッサ u が行うプロセッサ v の検査を有向辺 (u,v) で表すことによって有向グラフで表すことができる．このグラフを検査割当グラフと呼ぶ．D を検査割当グラフとする．また, 検査結果は検査割当グラフの有向辺集合から $\{0,1\}$ への写像 σ として表すことができる．σ をシンドロームと呼ぶ．故障プロセッサ数が t を越えないという仮定の下で, D 上の任意のシンドロームに対して全ての故障プロセッサを一意に同定できるならば, D は t-診断可能であると言われる．Hakimi と Amin [2] は D が t-診断可能であるための必要十分条件を示した．

PMC モデルは次の 2 つの現実的な問題を考慮していない: (1) プロセッサが故障診断の最中に故障するかもしれない．(2) 故障が断続的であるかもしれない．これらの問題を考慮するために, Fu と Beigel [1] は PMC モデルを以下のように拡張した: プロセッサは正常, 常時故障, 断続的故障のいずれかの状態をとり, 故障診断の最中にこの状態が変わることはないと仮定する．また, 任意のプロセッサが断続的故障プロセッサを検査した場合も, 断続的故障プロセッサが任意のプロセッサを検査した場合も, 検査結果は 0 もしくは 1 であるとする．Fu と Beigel によるこのモデルを FB モデルと呼ぶ．断続的故障プロセッサは, 故障診断の間正常なプロセッサと同じ振舞いをすることがあり得るため, 同定することを保証できない．そこで, 診断可能性を以下のように定義する: 断続的故障プロセッサ数が s を, 常時および断続的故障プロセッサの数が t を越えないという仮定の下で, D 上の任意のシンドロームに対して全ての常時故障プロセッサを含む集合と全ての正常プロセッサを含む集合から成るプロセッサ集合の分割を与えることができるならば, D は (s,t)-診断可能であると言われる．

本研究では, D が (s,t)-診断可能であるための必要十分条件を示す．また, D が (t,t)-診断可能であるときに, 任意のシンドロームに対して全ての常時故障プロセッサを含む集合と全ての正常プロセッサを含む集合から成るプロセッサ集合の分割を与える線形時間アルゴリズムを示す．

2. 準備

D を有向グラフとし, $V(D)$ と $E(D)$ をそれぞれ点集合と有向辺集合とする．任意の $v \in V(D)$ に対して

$$\Gamma^-_D(v) = \{u : (u,v) \in E(D)\}, \quad \delta^-_D(v) = |\Gamma^-_D(v)|$$
$$\Gamma^+_D(v) = \{u : (v,u) \in E(D)\}, \quad \delta^+_D(v) = |\Gamma^+_D(v)|$$

とする．また, 任意の $X \subseteq V(D)$ に対して

$$\Gamma^-_D(X) = \bigcup_{v\in X} \Gamma^-_D(v) - X, \quad \delta^-_D(X) = |\Gamma^-_D(X)|$$
$$\Gamma^+_D(X) = \bigcup_{v\in X} \Gamma^+_D(v) - X, \quad \delta^+_D(X) = |\Gamma^+_D(X)|$$

とする．さらに,

$$\delta^-(D) = \min_{v\in V(D)} \delta^-_D(v), \quad \delta^+(D) = \min_{v\in V(D)} \delta^+_D(v)$$

とする．

σ を D 上のシンドロームとする． すなわち, $\sigma : E(D) \to \{0,1\}$ とする．$V(D)$ の分割 (H,I,P) は次の 2 つの条件を満たすならば σ に矛盾しないと言われる．

- $u,v \in H, (u,v) \in E(D) \Rightarrow \sigma(u,v) = 0;$

† 埼玉大学 Saitama University

- $u \in H, v \in P, (u,v) \in E(D) \Rightarrow \sigma(u,v) = 1$.

逆に, σ は (H,I,P) に矛盾しないとも言う.

$|I| \leq s$ かつ $|P|+|I| \leq t$ であるような $V(D)$ の任意の分割 (H,I,P) と, (H,I,P) に矛盾しない任意のシンドローム σ に対して, $P \subseteq F \subseteq P \cup I$ を満たす F を見つけるアルゴリズムを (s,t)-故障診断アルゴリズムと呼ぶ. (s,t)-故障診断アルゴリズムが存在する D は (s,t)-診断可能であると言われる.

3. (s,t)-診断可能性

$|I| \leq s$ かつ $|P|+|I| \leq t$ であるような σ に矛盾しない $V(D)$ の分割 (H,I,P) から成る集合を $\mathcal{D}_D(\sigma,s,t)$ で表す. 以下の定理は簡単に示される.

定理 1 D が (s,t)-診断可能であるための必要十分条件は, 次の条件を満たすことである: $\mathcal{D}_D(\sigma,s,t) \neq \emptyset$ である任意のシンドローム σ と, σ に矛盾しない $V(D)$ の任意の分割 (H_1,I_1,P_1) と (H_2,I_2,P_2) に対して, $H_1 \cap P_2 = \emptyset$ かつ $P_1 \cap H_2 = \emptyset$ である.

定理 2 s,t を $s \leq t$ を満たす正の整数とする. D が (s,t)-診断可能であるための必要十分条件は, 次の 3 つの条件を満たすことである：

(1) D の点数 $n \geq 2t+1$;

(2) $\delta^-(D) \geq t+s$;

(3) 各整数 p $(0 \leq p \leq t-s)$ と各 $X \subseteq V(D)$ $(|X| = n-2t+p)$ に対して $\delta^+_D(X) > p+2s$.

証明： 紙面の都合上, 必要条件の証明は省き, 十分条件のみを示す.

背理法により D は (1)(2)(3) の条件を満たすとし D は t-診断可能でないと仮定する. このとき, あるシンドローム σ に対して, $P_1 \cap H_2 \neq \emptyset$, $|I_1|, |I_2| \leq s$ かつ $|I_1 \cup P_1|, |I_2 \cup P_2| \leq t$ であるような二つの矛盾しない $V(D)$ の分割 (H_1,I_1,P_1) と (H_2,I_2,P_2) が存在する. まず, $n-2t \leq |H_1 \cap H_2| < n-t-s$ であることを示す.

$f = |(I_1 \cup P_1) \cap (I_2 \cup P_2)|$ とする. このとき, $|H_1 \cap H_2| = n - |I_1 \cup P_1| - |I_2 \cup P_2| + f \geq n-2t+f \geq n-2t$ である.

$|H_1 \cap H_2| \geq n-t-s$ と仮定する. 任意の $w \in P_1 \cap H_2$ について考える. ある $v \in H_1 \cap H_2$ に対して $(v,w) \in A(D)$ であると仮定する. (H_1,I_1,P_1) は σ に矛盾しないので, $\sigma(v,w) = 1$ である. また, (H_2,I_2,P_2) は σ に矛盾しないので, $\sigma(v,w) = 0$ である. これは矛盾であり, $(v,w) \notin A(D)$ である. したがって, $\Gamma^-_D(w) \subseteq V(D) - (H_1 \cap H_2) - \{w\}$ であり, $\delta^-_D(w) \leq n-(n-t-s)-1 = t+s-1$ となる. これは条件 (2) に矛盾する. よって, $|H_1 \cap H_2| < n-t-s$ である.

以上のことから, $|H_1 \cap H_2| = n-2t+p$ であるような整数 $p (0 \leq p < t-s)$ が存在する. $|H_1 \cap H_2| \geq n-2t+f$ であるので, $f \leq p$ である. また, 前述の議論より $\Gamma^+_D(H_1 \cap H_2) \subseteq ((I_1 \cup P_1) \cap (I_2 \cup P_2)) \cup (I_1 \cap H_2) \cup (H_1 \cap I_2)$ であるので, $\delta^+_D(H_1 \cap H_2) \leq f + |I_1| + |I_2| \leq p+2s$ となる. これは条件 (3) に矛盾する. よって, D は (s,t)-診断可能である. （証明終）

4. 故障診断アルゴリズム

D を (t,t)-診断可能である有向グラフとする. 定理 2 より $\delta^-(D) \geq 2t$ であることに注意されたい. このとき, D に対する (t,t)-故障診断アルゴリズムを以下に示す.

```
function (t,t)-fault-diagnosis(D, σ, t)
{
  F = ∅
   for(∀v ∈ V(D)){
      if (|{u : σ(u,v) = 1}| ≥ t + 1)
        then F ← F ∪ {v};
   }
  return(F);
}
```

図 1　故障診断アルゴリズム

5. まとめ

本研究では, D が (s,t)-診断可能であるための必要十分条件を示した. また D が (t,t)-診断可能であるときに, D に対する (t,t)-故障診断アルゴリズムを与えた. 今後の課題は D が (s,t)-診断可能であるときに, (s,t)-故障診断アルゴリズムを与えることである.

参考文献

[1] Bin Fu and Richard Beigel. Diagnosis in the presence of intermittent faults. *Lecture Notes in Computer Sciences*, 3341:427–441, 2004.

[2] S.L. Hakimi and A.T. Amin. Characterization of connection assignment of diagnosable systems. *IEEE Transcations on Computers*, 23:86–88, 1974.

[3] F.P. Preparata, G. Metze, and R.T. Chien. On the connection assignment problem of diagnosable systems. *IEEE Transactions on Electronic Computers*, 16:848–854, 1967.