不完全 Self-checking Network에 있어서의 데이터信賴度

論 文
27~4~1

Data Reliability in a Partially Self-checking Network

吳 永 敦*
(Young Don Oh)

Abstract

Intermittent failures exercise their effects only part of the time but constitute a dominant factor for the field failures.

We consider the data reliability of the partially self-checking network with which a single intermittent failure will be recovered by a rollback method. Even if the self-testingness of partially self-checking network is guranteed for a set of permanent failures, it sometimes may not be so for intermittent failures.

We introduce the notion of error residual and provide the basis for calculating the data reliability. Both the duration of each intermittent failure and the occurrence interval of successive ones are assumed to be negative exponentially distributed; the convolution of the intervals is distributed according to an Erlangen distribution.

Ⅰ. 서 론

計算機시스템에 있어서 하아드웨아上의 고장이 발생하면, 프로그램을 바르게 遂行할 수 없게 되어 計算結果에 에러를 포함하게 된다.

이러한 에러의 원인이 되는 고장을 그 물리적 성질에 따라 대별하면, 機能에 永久的變化를 가져오는 永久故障(Permanent failure, solid failure)과 그렇지 않는 間歇故障(intermittent failure, transient failure)의 두가지로 된다. 間歇故障은 그 발생원인이 복합적이고[1], 어떤 짧은 시간 동안 永久故障과 동일한 장해를 주나, 그 고장이 자연소멸된 후에는 고장의 흔적을 남기지 않는다.

고장을 신속히 제거하기 위해서는 고장에 대한 檢出이 선행해야 하므로, Carter[2]와 Anderson[3]은 回路의 出力을 에러檢出符號化하고 여기에 符號檢出器를 설치한 self-checking network(SCN)를 고안하였다. SCN은 self-testing과 fault-secure의 두가지 성질을 가지고 있다. 즉, 임의의 고장 $f^* \in F$(F는 고장의 集合)를 검출케 하는 入力$X \in N$(N은 넷워크의 許容入力의 集合)가 있을 때, 이 넷워크는 self-testing이라고 하고, 모든 고장 $f \in F$에 대하여, 검출이 가능하거나, 그렇지 않으면 無故障時와 같은 出力을 낼 때, 이넷워크를 fault-secure라 한다. 넷워크가 self-testing과 fault-secure의 두 성질을 겸비할 때 完全SCN이라 하고, fault-secureness가 불완전할 때, 이것을 不完全SCN이라 한다.

고장 $f \in F$를 갖는 不完全SCN[4],[5]에 入力$X \in N$가 가해지면, 出力에서 고장 f를 檢出(D : Detection) 하거나, 혹은 出力이 에러(E : Error)임에도 이것을 판별못하거나, 혹은, 無故障時와 같은 바른 出力(C : Correct response)을 내게 된다.

즉, 고장 $f \in F$가 있을 때, 바른 出力 C를 내는 確率을 $c = \Pr(C|f)$, 같은 모양으로 $d = \Pr(D|f)$, $e = \Pr(E|f)$라고 하면

* 正會員 : 日本 東京工業大學工學部 客員研究員
接受日字 : 1978年 6月 5日

* 以下에 있어서 f는 永久故障을 가르키는 것으로 한다.

$c=\Sigma_j: X_j \epsilon N_C \Pr(X_j)$

$d=\Sigma_j: X_j \epsilon N_D \Pr(X_j)$

$e=\Sigma_j: X_j \epsilon N_E \Pr(X_j)$

를 만족하는, 入力의 集合 N의 部分集合 N_C, N_D, N_E가 있고

$N_C \cup N_D \cup N_E = N (N_C \cap N_E = N_C \cap N_D = N_D \cap N_E = \phi)$

$c+d+e=1$

이 된다.

이러한 c, d, e의 값은 시뮬레이션에 의하여 실험적으로 구해지는데, 거동이 불확실한 間歇故障 대신 永久故障을 人爲的으로 삽입하여 그 값을 정한다. 따라서 c, d, e의 값에 관한 한, 永久故障에 대한 값을 나타내고 있다.

完全SCN에서는 모든 고장 $f \in F$에 대하여 $d>0$, $e=0$이고, 不完全SCN에서는 어떤 고장 $f \in F$에 대하여 $d>0$, $e>0$이므로, 完全SCN이 바람직하나, 回路의 集積度가 향상되어 그 기능이 복잡화 할 수록 $e=0$이 되는 完全SCN은 기술적으로 설계가 곤란하게 되었다[6]. 따라서 不完全SCN이 일반적이라고 보는 것이 타당하다.

한편 計算機의 이용면에 있어서는 더욱 계산의 정확도가 요구되어, 에러除去에 대한 방법을 중요시하게 되었다. 에러의 원인이 되는 고장을, 그 발생빈도 면에서 비교하면, 間歇故障은 計算機出荷前의 故障率의 30%, 현장에서의 고장의 90%를 점하고 있다.[7] 따라서 間歇故障에 대한 대책이 중요하며, 여기에 rollback recovery(RR)法이 있고, retry는 그 축소형이라 할 수 있다.

RR는 아래와 같은 4단계로 구성되어 있다.

i) 計算의 中間結果 및 그 당시의 여러 정보(status vector)를 一定間隔 혹은 非一定間隔으로 補助記憶裝置에 save 한다(checkpointing).

ii) 計算途中에 고장이 검출되면, 계산을 중단하고 save해 둔 最新의 정보를 主記憶裝置에 load 한다.

iii) ii)가 끝난 상태에서 같은 계산을 再實行한다.

iv) 처음 고장이 검출된 곳에서 다시 고장이 검출되면, 永久故障으로 판단하여 永久故障對策을 취한다. 고장의 再檢出이 없으면 발생했던 間歇故障은 해소되었고, 그 고장으로 인하여 발생했을지도 모르는 에러도 제거되었다고 판단한다.

그러나, 間歇故障으로 인한 에러를 不完全SCN의 도움을 받아 RR할라고 할 때, 자연히 그 달성도에 제한을 받게 된다.

본 논문은 이러한 제한의 원인을 규정짓고, 이에 의하여 데이터의 信賴度 및 어떠한 신뢰도가 요구될 때의 不完全SCN의 조건 등을 고찰해 보기로 한다.

2. 모델 및 假定

間歇故障과 rollback recovery에 관하여 다음과 같이 정한다.

a 間歇故障에 대하여

i) 發生數는 Poisson分布에, 즉, 그 發生間隔은 指數分布에 따른다.

ii) 間歇故障의 繼續時間은 平均값 $\bar{D}=22\mu s$인 指數分布에 근사적으로 따른다.

iii) 一時에 발생하는 고장의 수는 단 1개, 즉 單一故障만을 고려한다.

iv) 1클록間隔 $\Delta(10^{-7}s$로 봄)에 있어서는, 間歇故障도 永久故障과 동일하게 취급한다.

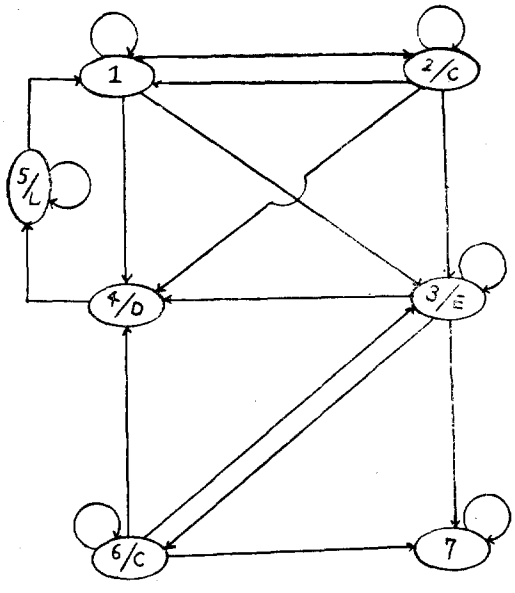
b. rollback recovery에 대하여

i) save나 load에 일정시간을 요하며, 이 시간 $T_S(=T_L) \gg \bar{D}$이다.

위의 a의 ii)에 대하여 좀 더 설명하기로 한다. 일반적으로 間歇故障은 一定遷移率을 갖인 2狀態마아코프 모델에 의하여 나타내기도 하나[8], 결정적인 견해는 없다. 특히 결정짓기 어려운 계속시간 $\tilde{t}$에 대하여, 본 논문에서는 $t_f \leq \tilde{t} \leq t_f+\alpha$($t_f$: 고장발생시간, $\alpha=10 \sim 100\mu s$)[9]에서 上限값으로서 $100\mu s$[10]를 취하기로 하고, 그 繼續如何의 不規則性으로 보아 指數分布에 따른다고 가정한다. 이와 같은 가정을 근사적으로 만족하는 指數分布를 구하기 위하여 $\int_0^{100} \gamma \exp(-\gamma x)dx = 0.99$를 풀면, $\bar{D}=1/\gamma \fallingdotseq 22\mu s$가 된다.

3. 不完全SCN의 에러殘留度 및 데이터의 信賴度

不完全SCN에 間歇故障이 있을 때, 그 出力의 양상과 RR에 의한 에러除去過程을 그림 1에 나타내고 있다. 狀態 5를 제외하고는 1클록 Δ마다 상태를 변할 수 있다. 상태 5에서는 load에 필요한 일정시간을 소요한 후에 상태 1에 도달한다. 상태 3이나 6에 있다가, 다음 순간(클록)에 고장이 $\gamma\Delta$의 확률로 자연소멸되면 상태 7에 이르고, 일단 이 상태에 이르면, 프로그램을 처음부터 다시 시작해서, 인위적으로 상태 1로 복귀시키지 않는 한, 다른 상태로 옮아갈 수 없다. 한편, 상태 2에 있다가 확률 $\gamma\Delta$로 고장이 자연 소멸되면, 상태 1에 복귀하게 되고, 이때에는 아무 고장이 없을 때와 결과적으로 같게 된다.



상태 1 : 無故障, 無에러
상태 7 : 無故障이나, 回復不可能한 에러포함
상태 2,3,6 : 상태 1에도, 상태 7에도 갈 수 있는 과도상태
상태 4 : 즉시 상태 5로 옮김
상태 5 : load

그림 1. 間歇故障을 갖는 不完全SCN의 狀態遷移
Fig. 1. Transitions in a partially self-checking network with an intermittent failure

그림 1에서 보는 바와 같이 不完全SCN에 間歇故障이 있을 때 상태 7에 이른다는 것은 중요한 의미를 가진다.

間歇故障은 有限時間 동안 永久故障과 같이 거동한다는 뜻에서, $f'\in F$로써 나타내고, f'로 인한 에러로부터의 회복수단으로서 RR을 가정할 때, 아래와 같은 정의를 한다.

〔定義〕 不完全SCN($d>0$, $e>0$)에 間歇故障 $f'\in F$가 있을 때, 回復不可能한 에러를 발생하는 확률을 不完全SCN의 에러殘留度라 한다.

다음에 에러殘留度 p를 구해 본다.

p는 그림 1에서 상태 3이나 6에 있다가 상태 7로 옮기는 확률이다. 즉, 길이 n되는 出力의 有限系列 중에 E가 하나 이상 들어 있고, D는 없는 확률이 된다. 먼저 n을 一定으로 하고, E, D의 발생횟수를 E', D'로 나타내면

$$\Pr(E'\geq 1,\ D'=0 \mid f') = \Pr(E'\geq 1 \mid f',\ D'=0)\Pr(D'=0 \mid f') = [1-\Pr(E'=0 \mid f',\ D'=0)]\Pr(D'=0 \mid f') = \left[1-\left(\frac{c}{c+e}\right)^n\right](c+e)^n \quad (1)$$

이고, 고장의 계속시간 $n\Delta$는 指數分布에 따르는 確率變數이므로

$$p=\sum_{n=1}^{1000}\left[1-\left(\frac{c}{c+e}\right)^n\right](c+e)^n\Pr(n\Delta)$$

$$\fallingdotseq\sum_{n=1}^{\infty}[(c+e)^n-c^n]\gamma\Delta\exp[-n\gamma\Delta]$$

$$=\frac{e\gamma\Delta\exp[-\gamma\Delta]}{[1-(c+e)\exp[-\gamma\Delta]][1-c\exp[-\gamma\Delta]]}$$

또, $\gamma=0.046/10^{-6}$sec, $\Delta=10^{-7}$sec를 취하였으므로, $\gamma\Delta=0.0046$이고, 이때 $\exp[-\gamma\Delta]\fallingdotseq 1$이 되어 아래와 같이 된다. 즉

$$p=\frac{e}{(1-c)d}\gamma\Delta \quad (3)$$

식 (3)에서 p의 값이 e/d에 비례함은 쉬 알 수 있으나, $(1-c)$에 反比例한다는 사실에 주의를 요한다. c는 maskability라고도 하며, 고장이 있음에도 불구하고 이 고장이 차폐(mask)되어 出力이 正常時와 같게 되는 확률이다. 따라서 이 값이 클수록 p의 값은 작을 것으로 생각되나, 반드시 그렇지 않음을 나타내고 있다. 식 (3)은 間歇故障이 빈발하는 환경에서 不完全SCN을 사용하고져 할 때, 不完全SCN을 평가하는 하나의 기준이 될 것이다.

다음에 p의 값이 정해진 不完全SCN을 이용하여 rollback recovery를 할 때, t時間後의 계산결과의 신뢰도에 대하여 고찰하기로 한다. 이 때, 고장은 save나 load 중에는 발생하지 않으며, 또 계산을 시작하는 $t=0$에서는 고장은 없다고 가정한다.

回復不能인 에러가 발생하기까지의 시간을 T라고 하면, 시간 t에 있어서의 데이터의 信賴度 R는 아래와 같다.

$$R=\Pr(T>t)=1-\Pr(T\leq t) \quad (4)$$

고장이 패러미터 τ인 Poisson分布에 따라 발생하게 되면, 그 발생간격 Z_i는 平均 $1/\tau$인 指數分布에 따르게 되고, k회 발생했을 때의 總間隔은 $Y_k=\Sigma_{i=1}^{k}Z_i$가 된다. 한편, Y_k는 確率密度函數가

$$f(t)=\begin{cases}\dfrac{\tau^k t^{k-1}}{(k-1)!}\exp[-\tau t] & t>0\\ 0 & t<0\end{cases}$$

인 Erlangen分布에 따르게 됨이 알려져 있다.[11]

따라서 식 (4)는 k가 一定할 때

$$\Pr(T>t) = \Pr(Y_k>t)\ (1-p)^{k-1}p \quad (5)$$

가 된다.

그런데 $k=1,2,3,\cdots\cdots$이므로

$$R=\sum_{k=1}^{\infty}\Pr(Y_k>t)\ (1-p)^{k-1}p \qquad (6)$$

이 되며, 여기서

$$\Pr(Y_k>t)=\int_t^{\infty}\frac{\tau^k u^{k-1}}{(k-1)!}\exp[-\tau u]du$$

$$=\sum_{r=0}^{k-1}\frac{(\tau t)^r}{r!}\exp[-\tau t]$$

이므로

$$R=\sum_{k=1}^{\infty}\sum_{r=0}^{k-1}\frac{(\tau t)^r}{r!}\exp[-\tau t](1-p)^{k-1}p$$

$$=\exp[-\tau t]\sum_{m=0}^{\infty}\frac{[\tau t(1-p)]^m}{m!}$$

$$=\exp[-p\tau t] \qquad (7)$$

이다.

거꾸로, 시간 t, 패러미터 τ 및 신뢰도 $R\geq\beta$가 주어졌을 때, 不完全SCN의 p의 값은 아래와 같이 된다.

즉 $\exp[-p\tau t]\geq\beta$(가령 0.99)이라면

$$p\leq\frac{-1}{\tau t}ln\beta \qquad (8)$$

4. 결　론

計算機의 고장에 관하여는 永久故障보다 間歇故障이 빈번히 발생하고 있음에도 불구하고, 間歇故障의 거동의 不規則性 때문에, 이 문제에 대한 연구가 미루어져 왔다. 근간에 間歇故障에 대한 off-line test [8],[1]에 관한 연구가 시작되었고, 현재 진행중에 있다.[12],[13] 한편 on-line recovery에 관하여는 checkpointing間隔의 最適化[14],[15]에 관한 연구가 있으나, 데이터의 신뢰도에 관한 것은 별로이 볼 수 없다. 본 논문은 不完全SCN의 에러殘留度의 개념을 도입하여, 間歇故障時에 문제가 되는 에러를 定量化하는데 기초를 세우고 이것을 이용하여 計算中의 임의시각에 있어서의 데이터의 신뢰도를 검토하였다.

앞으로 남은 문제는 모델의 정밀화와 확장, 그리고 永久故障과 間歇故障이 공존하는 상태에서, 에러殘留度를 고려한 효과적인 시스템의 구성방법 등이 남아 있다.

참 고 문 헌

1. S. Kamal, "An approach to the diagnosis of intermittent faults," IEEE Trans Comput. vol C-24, May 1975.
2. W.C. Carter and P.R. Schneider, "Design of dynamically checked computers," 1968. Proc IFIP Congr. vol.2, North Holland.
3. D.A. Anderson and G.Metze, "Design of totally self-checking check cercuits for m-out-of-n codes," IEEE Trans. comput vol C-22, Mar 1973.
4. J.F. Wakerly, "Partially self-checking circcuits and their use in performing logical operations," IEEE Trans, Comput, vol C-23 Jul. 1974.
5. J.J. Shedletsky, "A rollback interval for networks with an imperfect self-checking properety," Dig. FTC-6, Jun. 1976.
6. F.A. Gay, "Reliability of partially self-checking circuits," Dig. FTC-7, Jun 1977.
7. M. Ball and F. Hardie, "Effects and detection of intermittent failures in digital systems," FJCC, AFIPS Proc vol.35, 1969.
8. M.A. Breuer, "Testing for intermittent faults in digital circuits," IEEE Trans Comput, vol C-22, Mar. 1973.
9. W.C. Carter, Computer Systems Reliability, p.417, 1974 Infotech Information Ltd. England
10. A. Avizienis, Computer Systems Reliability, p. 225, 1974 Infotech Information Ltd. England
11. D.R Cox, Renewal Theory, p.15, 1962, Methuen & Co Ltd.
12. R.J. Spillman, "A markov model of intermittent faults in digital systems," Dig. FTC-7 Jun 1977.
13. J. Savir, "Optimal testing of single intermittent failures in Combinational circuits," Dig FTC-7, Jun 1977.
14. K.M. Chandy and C.V. Ramamoorthy, "Rollback recovery strategies for computer programs," IEEE Trans Comput vol C-21, Jun, 1972
15. K.M. Chandy, J.C. Brown, C.W. Dissly and W.R. Uhrig, "Analitic models for rollback and recovery strategies in data base systems," IEEE Trans Software engineering vol SE-1 Mar. 1975

謝辭 본 연구를 수행하는데 있어서 적절한 지도와 격려를 하여주신 서울大學校工科大學의 梁興錫敎授님께 감사드리며, 또한 본 논문의 내용개선을 위하여 여러가지 긴요한 점을 지적하여 주신 審査委員에게 謝意를 표합니다.