Kullback-Leiblerの情報量に基づくソフトウェアのゼロ障害型信頼性実証試験

5G－8

澤田　清　　三道　弘明
流通科学大学情報学部

1. はじめに

信頼性実証試験[1] (Reliability Demonstration Testing) は，ハードウェア製品の開発段階終了後，そのハードウェアに目標とする信頼性が十分に実現されているかどうかの実証・確認を目的として考案された．ソフトウェアの品質保証が問題となっている今日，ソフトウェア製品に対してもこの信頼性実証試験の考え方を適用することは十分に意義のあることである．

このような考え方に基づき，筆者らは，これまでハードウェアに対して提案されてきた信頼性実証試験の種々の方法のうち，規準型およびゼロ障害型の試験方法をソフトウェアに適用することを試みた[2]~[4]．規準型の信頼性実証試験では，ハードウェアに対するそれと同様に，統計的検定論の考え方に基づいて，生産者リスクと消費者リスクの値を指定する方法により定式化した．一方，あらかじめ定められた試験中に発生した障害回数が0のときのみ対象製品を合格とするゼロ障害型の信頼性実証試験においては，設計変数が1つだけであるので，生産者リスクまたは消費者リスクのどちらか一方の値を指定することにより設計可能であった．なお，対象としては，計算機のＯＳや生産システムの制御ソフトウェアのように時間に関して連続的に用いられるソフトウェア[2],[3] (以後，連続型ソフトウェアと呼ぶ) と，通常の数値計算ソフトウェアのように時間に関して離散的に使用されるソフトウェア[4] (以後，離散型ソフトウェアと呼ぶ) の2通りを考えた．

本研究では，ソフトウェアのゼロ障害型信頼性実証試験に対して，Kullback-Leiblerの情報量[5],[6]を用いた新しい設計方法を提案する．なお，ここでも，連続型および離散型の2通りのモデルを扱う．

2. Kullback-Leiblerの情報量と分離情報量

2つの確率分布 $F_1(x)$, $F_2(x)$ の密度関数をそれぞれ $f_1(x)$, $f_2(x)$ とするとき

$$I(F_1|F_2) = \int_0^\infty f_1(x) \log \frac{f_1(x)}{f_2(x)} dx \qquad (1)$$

を Kullback-Leibler の情報量という[5],[6]．ここで，$f_2(x) \propto$ constant とすると，$-I(F_1|F_2)$ はエントロピーを表す．

式(1)の $I(F_1|F_2)$ は，確率変数 X の値を観測することが，分布 $F_2(x)$ に比べ，$F_1(x)$ に対して提供する情報量を意味する．

ここで

$$J(F_1,F_2) \equiv I(F_1|F_2) + I(F_2|F_1) = \int_0^\infty [f_1(x) - f_2(x)] \log \frac{f_1(x)}{f_2(x)} dx \qquad (2)$$

なる量を考えると $J(F_1,F_2) = J(F_2,F_1)$ が成り立ち，これを分離情報量 (divergency) と呼ぶ[6]．式(2)の分離情報量は，分布 $F_1(x)$, $F_2(x)$ に対する重みを対等とみなした場合の情報量であると考えることができる．

また，離散型分布に対する Kullback-Leibler の情報量および分離情報量は，それぞれ次のように表される．

$$I(F_1|F_2) = \sum_{i=0}^{\infty} p_{1i} \log \frac{p_{1i}}{p_{2i}} \qquad (3)$$

$$J(F_1,F_2) = \sum_{i=0}^{\infty} [p_{1i} - p_{2i}] \log \frac{p_{1i}}{p_{2i}} \qquad (4)$$

ただし，p_{1i}, p_{2i}は，$X = x_i (i = 0,1,2,\cdots,\infty)$ となる確率を表す．

3. 連続型モデル

前述したような時間に関して連続的に利用されるソフトウェアに対して，次のようなゼロ障害型信頼性実証試験を考える．すなわち，対象ソフトウェアを現実の使用環境のもとで予め定められた t 時間だけ試験し，試験期間中に生起したソフトウェア障害回数が0の場合のみそのソフトウェアを合格とし，1回でも障害が発生すれば不合格とする．このとき，$t(t>0)$ の値をいかに設定するかが問題である．

ここで，ソフトウェアの生産者（開発者）がその開発を受注したときのソフトウェアの平均ソフトウェア障害時間間隔 MTBSF(Mean Time Between Software Failures) に対する契約の値，および消費者（ユーザ）が受け入れ可能な MTBSF の下限値をそれぞれ θ_0, θ_1と書くことにする ($\theta_0 \geq \theta_1$)．さらに，t時間の試験中にソフトウェア障害が1回以上発生するという事象を E_1，E_1の排反事象を$\overline{E_1}$と書くこととする．なお，ここでは，ソフトウェア障害の時間間隔は平均 θ の指数分布に従うものとする．

このとき，対象ソフトウェアの真の MTBSF が契約の値θ_0であるときに，事象 E_1，$\overline{E_1}$が起こる確率は，それぞれ

$$Pr[E_1|\theta_0] = 1 - \exp(-t/\theta_0) \qquad (5)$$

Zero-Failure Software Reliability Demonstration Testing based on Kullback-Leibler Information
Kiyoshi Sawada　Hiroaki Sandoh
University of Marketing & Distribution Sciences
3-1 Gakuen-nishi-machi, Nishi-ku, Kobe 651-21, Japan

$$Pr[\overline{E_1}|\theta_0] = \exp(-t/\theta_0) \quad (6)$$

となる．また，対象ソフトウェアの真のMTBSFが受け入れ可能な下限値θ_1であるときに，事象E_1，$\overline{E_1}$が起こる確率は，それぞれ

$$Pr[E_1|\theta_1] = 1-\exp(-t/\theta_1) \quad (7)$$

$$Pr[\overline{E_1}|\theta_1] = \exp(-t/\theta_1) \quad (8)$$

となる．

このとき，式(5)，(6)および式(7)，(8)は，それぞれ，E_1，$\overline{E_1}$という2つの事象からなる離散型確率分布となるので，これらの分布の分離情報量が最も大きくなる（2つの確率分布が最も弁別される）ようなtを選べば，真のMTBSFに対して誤った試験結果を下す可能性が最も小さいこととなる．

上述した2つの分布の分離情報量は

$$J(F_1,F_2) = [\exp(-t/\theta_0)-\exp(-t/\theta_1)] \log\frac{\exp(-t/\theta_0)[1-\exp(-t/\theta_1)]}{\exp(-t/\theta_1)[1-\exp(-t/\theta_0)]} \quad (9)$$

であるから，これを最大にするようなtを求めればよい．

4. 離散型モデル

ソフトウェアが必要とする一組の入力変数の値の集合を単に入力と呼ぶこととすると，離散型ソフトウェアの信頼度は，次のように定量的に定義することができる．すなわち，対象ソフトウェアに対する可能な入力の数をN，そのうちソフトウェア障害を生起させる入力数をN_0と表すこととする．このとき，N個の可能な入力から任意に選んだ1つの入力に対して，ソフトウェア障害が生起する確率はN_0/Nで与えられる．なお，通常N，N_0の値は非常に大きく，天文学的な数値となる．前述の確率をpで表すと，pは対象ソフトウェアの不信頼度を表すと解釈することができる．

このような性質を有するソフトウェアに対して，次のようなゼロ障害型信頼性実証試験を考える．すなわち，N個の中から任意に選んだn個の入力を用いて対象ソフトウェアを試験し，ソフトウェア障害を引き起こした入力の数が0の場合のみそのソフトウェアを合格とし，1つでも障害を引き起こす入力があれば不合格とする．このとき，$n(n=1,2,\cdots)$の値をいかに設定するかが問題である．

ここで，ソフトウェアの生産者（開発者）がその開発を受注したときのソフトウェアの不信頼度に対する契約の値，および消費者（ユーザ）が受け入れ可能な不信頼度の上限値をそれぞれp_0，p_1と書くこととする$(p_0 \le p_1)$．さらに，n個の入力を用いた試験中に，ソフトウェア障害を引き起こす入力が1以上あるという事象をE_2，E_2の排反事象を$\overline{E_2}$と書くこととする．

このとき，対象ソフトウェアの真の不信頼度が契約の値p_0であるときに，事象E_2，$\overline{E_2}$が起こる確率は，それぞれ

$$Pr[E_2|p_0] = 1-(1-p_0)^n \quad (10)$$

$$Pr[\overline{E_2}|p_0] = (1-p_0)^n \quad (11)$$

となる．また，対象ソフトウェアの真の不信頼度が受け入れ可能な上限値p_1であるときに，事象E_2，$\overline{E_2}$が起こる確率は，それぞれ

$$Pr[E_2|p_1] = 1-(1-p_1)^n \quad (12)$$

$$Pr[\overline{E_2}|p_1] = (1-p_1)^n \quad (13)$$

となる．

このとき，式(10)，(11)および式(12)，(13)は，それぞれ，E_2，$\overline{E_2}$という2つの事象からなる離散型確率分布となるので，これらの分布の分離情報量が最も大きくなる（2つの確率分布が最も弁別される）ようなnを選べば，真の不信頼度に対して誤った試験結果を下す可能性が最も小さいこととなる．

上述した2つの分布の分離情報量は

$$J(F_1,F_2) = [(1-p_0)^n-(1-p_1)^n] \log\frac{(1-p_0)^n[1-(1-p_1)^n]}{(1-p_1)^n[1-(1-p_0)^n]} \quad (14)$$

であるから，これを最大にするようなnを求めればよい．

ここでは，ページ数の関係上数値例は割愛することとし，当日報告させて頂く．

文献

(1) Mann, N.R., R.E. Schafer and N.D. Singpurwalla: *Methods for Statistical Analysis of Reliability and Life Data*, Wiley, New York, 1974, pp.404-410.

(2) 三道弘明，澤田　清：“ソフトウェアに対するゼロ障害型信頼性実証試験に関する研究”，電子情報通信学会論文誌 (A), J73-A, 3, 1990, pp.564-569.

(3) Sandoh, H.: “Reliability demonstration testing for software,” *IEEE Trans. Reliability*, Vol.R-40, 1991, pp.117-119.

(4) Sandoh, H. and K. Sawada: “Reliability demonstration testing for discrete-type software products,” *Proc. of 1991 Annual Reliability and Maintainability Symp.*, Orland, Florida, 1991, pp.428-432.

(5) Kullback, S. and R.A. Leibler: “On information and sufficiency,” *Ann. Math. Statist.*, Vol. 22, 1951, pp.79-86.

(6) Kullback, S.: *Information Theory and Statistics*, Wiley, New York, 1959.