日本オペレーションズ・リサーチ学会
2004年秋季研究発表会

バリアントを選択する機能をもつ 3バージョンプログラミングシステムの信頼性評価に関する考察

法政大学大学院　田邊 朋哉 †　TANABE Tomoya
02101865　法政大学　木村 光宏 ††　KIMURA Mitsuhiro
01702425　鳥取大学　山田 茂 †††　YAMADA Shigeru

E-mail: †t-tomoya@pg8.so-net.ne.jp, ††kim@k.hosei.ac.jp, †††yamada@sse.tottori-u.ac.jp

1 はじめに

本研究では，フォールトトレラントソフトウェアシステムの一つである3バージョンプログラミングシステム [1] に焦点を当て，その信頼性を向上させる一手法について議論する．特に，システムに与えられた入力に基づいて3つのソフトウェアモジュール（バリアントと呼ぶ）が独立に生成した3つの処理結果において多数決が成立しないとき，過去のバリアントの出力結果と多数決の成立状況の記録から，いくつかの仮定の下で統計的に算出されるバリアントの優劣を表す量の推定値を用いて，その値が最も高いバリアントが生成した出力を，システム全体の出力とするシステムを提案する．また，そのシステムの信頼性特性について考察する．

2 3バージョンプログラミングシステム

まず，以下の諸量を定義する．

V_i: 第 i バリアント $(i = 1, 2, 3)$

p_i: V_i の信頼度 (V_i が期待通りの結果を出力する確率) $(0 \le p_i \le 1;\ i = 1, 2, 3)$

$\bar{p}_i$: $1 - p_i$ $(i = 1, 2, 3)$

a_i: V_i の期待通りでない出力が他のいずれかのバリアントの期待通りでない結果と一致しない確率を与えるパラメータ．つまり a_i はバリアント間の独立性を表すものとし，独立性パラメータと呼ぶ $(0 \le a_i \le 1)$.

また，以下の仮定をおく．

A1: ハードウェア故障は生じない．

A2: ボータにおける多数決決定は必ず正しく行われる．

A3: 1回の処理において各バリアントから出力された期待通りの結果は必ず一致する．

A4: 各バリアントはユーザ要求に照らして期待通りの出力かあるいは期待通りでない出力のいずれかをボータに渡す．

A5: 簡単のため，$a = a_1 = a_2 = a_3$ $(0 \le a \le 1)$ とする．

したがって，たとえば3つのバリアントが完全に独立であれば $(a = 1)$, 複数のバリアントが出力した期待通りでない結果は必ず一致せず，反対に $a = 0$ であれば複数のバリアントが期待通りでない結果を出力した場合，それらは必ず一致するものと仮定する．さて，上で述べたバリアントの独立性パラメータ を考慮すると，3つのバリアントからの出力により多数決が生ずる確率は $R + F_o(a)$ により表すことができる．ここで，R は2つあるいは3つの期待通りの出力結果により多数決が成立する確率，また $F_o(a)$ は期待通りでない出力どうしが一致することにより多数決が成立する確率をそれぞれ表している．具体的には，

$$R = p_1p_2p_3 + p_1p_2\bar{p}_3 + p_1\bar{p}_2p_3 + \bar{p}_1p_2p_3, \qquad (1)$$

および，

$$\begin{aligned} F_o(a) &= (1-a)^2[\bar{p}_1\bar{p}_2\bar{p}_3(1+2a) + (p_1\bar{p}_2\bar{p}_3 \\ &+ \bar{p}_1p_2\bar{p}_3 + \bar{p}_1\bar{p}_2p_3)], \end{aligned} \qquad (2)$$

である．

さらに，$F_n(a)$ を3つの出力結果が異なる確率とすれば

$$\begin{aligned} F_n(a) &= \bar{p}_1\bar{p}_2\bar{p}_3a^2(3-2a) + (p_1\bar{p}_2\bar{p}_3 \\ &+ \bar{p}_1p_2\bar{p}_3 + \bar{p}_1\bar{p}_2p_3)a(2-a), \end{aligned} \qquad (3)$$

となり，a にかかわらず $R + F_o(a) + F_n(a) = 1$ が成立する．

3 提案するシステム

本研究では，多数決決定を行うボータにバリアントの優劣を推定する機能をもたせることを提案する．具体的には、ボータが多数決決定の結果,「多数決が成立しない」との出力を行わざるを得ない場合に，ある評価基準の下で最も優れたバリアントから渡された出力をそのままシステムの出力とするシステムを提案する．

本節ではボータにおけるバリアントの優劣推定機能について述べ，システムの信頼性の解析を行う．

3.1 ボータによるバリアントの選択方法

3バージョンプログラミングシステムが繰り返し運用される場合を想定するとき，ボータは以下の互いに排反な5つの事象を観測することができる．

T_a: V_1 の出力が他の2つから孤立している．

T_b: V_2 の出力が他の2つから孤立している．

T_c: V_3 の出力が他の2つから孤立している．

T_d: すべての出力が一致している．

T_e: 多数決が成立しない．

システムが n 回動作したとき，ボータは上記の事象の生起回数を数えることができるとする．それらの観測値をそれぞれ C_a, C_b, C_c, C_d, および C_e とする ($C_a + C_b + C_c + C_d + C_e = n$)．この情報から，ボータはバリアントの信頼度を以下のように最尤法により推定する．いま，U_a,U_b,U_c,U_d, および U_e をそれぞれ事象 T_a, T_b, T_c, T_d, および T_e が発生する確率とする．このとき観測値に対する尤度関数 L は

$$L = \frac{n!}{C_a!C_b!C_c!C_d!C_e!} U_a^{C_a} U_b^{C_b} U_c^{C_c} U_d^{C_d} U_e^{C_e}, \quad (4)$$

で表される多項分布となる．これにより，同時対数尤度方程式を

$$\frac{\partial \log L}{\partial p_1} = 0, \ \frac{\partial \log L}{\partial p_2} = 0, \ \frac{\partial \log L}{\partial p_3} = 0, \quad (5)$$

とし，これらを数値的に解くことにより各バリアントの信頼度の最尤推定値 $\hat{p}_1$, $\hat{p}_2$, および $\hat{p}_3$ を求めることができる．本稿ではこれを各バリアントの優劣を表す量として用いることとする．また，推定における第1種および第2種の過誤の可能性があるため，ここに $P_{z_m}(m = 1, 2, 3)$ をボータによる1回の推定結果において，バリアント m の信頼度が他の2つのものより高いと推定する確率としておく．ここで $P_{z_1} + P_{z_2} + P_{z_3} = 1$ である．

3.2 システムの信頼度

以上により，バリアントの優劣推定機能をもつ3バージョンプログラミングシステムの信頼度 R_{sys} は

$$\begin{aligned} R_{sys} &= R + a(2-a)\{P_{z_1} p_1 \bar{p}_2 \bar{p}_3 + P_{z_2} \bar{p}_1 p_2 \bar{p}_3 \\ &+ P_{z_3} \bar{p}_1 \bar{p}_2 p_3\}, \end{aligned} \quad (6)$$

により与えられる．

3.3 P_{z_m} の振舞いと信頼度の上限

$P_{z_m}(m = 1, 2, 3)$ の値の振舞いについては，バリアントの信頼度 $p_m(m = 1, 2, 3)$ 間の値の差に支配されると考えられるが，解析的に求めることは困難であろう．

そこでいま，一般性を失うことなく3つのバリアントの真の信頼度が $p_1 \le p_2 \le p_3$ であると仮定し，b (> 0) を3つのバリアントの真の信頼度の差とする．すなわち，各バリアントの真の信頼度が

$$p_1 = p - b \ (> 0), \quad (7)$$
$$p_2 = p, \quad (8)$$
$$p_3 = p + b \ (< 1), \quad (9)$$

であるという仮定をおき，$P_{z_m}(m = 1, 2, 3)$ の値の振舞いについて調べることにする．p, b, および a の値を設定し，提案した3バージョンプログラミングシステムの動作をコンピュータシミュレーションしてみると，図1より P_{z_m} の値はバリアント間の信頼度の差 b と p の関係が，$b/(1-p) \ge 1/2$, つまり $b \ge \frac{1-p}{2}$ であるときにほとんど $P_{z_3} = 1$ となることが見て取れる．すなわち，この場合ボータが最尤法による推定を行った結果，真の信頼度が最も高いバリアントの選択に失敗することは稀である．また，p の値を変化させても P_{z_m} $(m = 1, 2, 3)$ の振舞いはほとんど変わらないことも見てとれる．

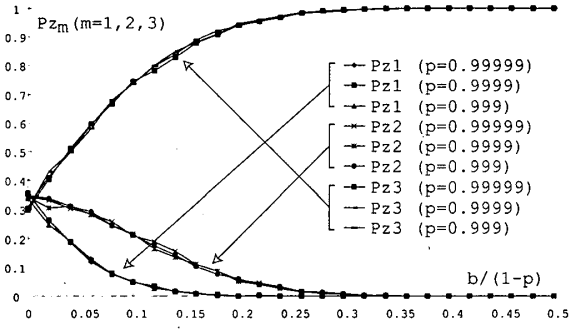

図1： P_{z_m} $(m = 1, 2, 3)$ の振舞い $(a = 0.5)$.

以上により，提案した3バージョンプログラミングシステムの上限 R_{sys}^{+} は，$1/2 \le b/(1-p) \le 1$ であるとき，$P_{z_3} = 1$, $P_{z_2} = 0$, $P_{z_1} = 0$ となると考え，さらにこのとき $p_1\bar{p}_2\bar{p}_3 < \bar{p}_1 p_2 \bar{p}_3 < \bar{p}_1\bar{p}_2 p_3$ が成立するので，

$$R_{sys}^{+} = R + a(2-a)(1-p+b)(1-p)(p+b), \quad (10)$$

により与えられる．

4 他のシステムとの比較

4.1 ランダム選択システム

前節で考察したバリアントの優劣を推定する機能をもつシステムに対して，最大信頼度を求めることなく，もし多数決決定が得られなかった場合は，ランダムにバリアントの出力を選んでシステムの出力とするというシステムも考えられる．このシステムを，ランダム選択システムと呼ぶことにする．この場合，システムの信頼度は

$$R_{ran} = R + a(2-a)\frac{1}{3}(p_1\bar{p}_2\bar{p}_3 + \bar{p}_1 p_2 \bar{p}_3 + \bar{p}_1\bar{p}_2 p_3), \quad (11)$$

となり，前節で仮定した条件 $p_1 = p - b$, $p_2 = p$, $p_3 = p + b$ の下では

$$R_{ran} = R + a(2-a)[b^2(\frac{2}{3} - p) + (1-p)^2 p], \quad (12)$$

となる．

4.2 信頼度の比較

いま，b と p の関係が $b/(1-p) \ge 1/2$, および $b > 0$ を満たすとすると，式 (10) の R_{sys}^{+} と式 (12) の R_{ran} との差は，$a > 0$ のとき

$$R_{sys}^{+} - R_{ran} = b(1 - p + \frac{b}{3}) > 0, \quad (13)$$

となることがわかる．したがってこの条件の下では，提案システムの信頼度はランダム選択のそれより大きくなることがわかる．

[1] L. L. Pullum, *Software fault tolerance: Techniques and implementation*, Artech House, Boston (2001).