モジュール間インタフェースの冗長化に着目したNバージョンプログラムの信頼性検討

3J－2

鈴木昭二　金川信康　佐藤美道　大辻信也
(株)日立製作所日立研究所

１．はじめに

ソフトウェア・フォールトトレラント技術の一つに，図１に示すようなNバージョンプログラムがある[2]．これは，同一仕様のもとで作成されたN個のバージョンの実行結果を多数決することによって，ソフトウェアのフォールト（バグ）をマスクするものである．しかし，本技法には開発／保守コストが多大になるという問題点がある．そこで本研究では，各バージョンを構成するモジュール同士を組み合せることにより，モジュール間のインタフェースの冗長化を行い，モジュール内のバグをマスクするといったNバージョンプログラムを提案する。本技法の信頼性検討の結果，更なる高信頼化・低コスト化を達成出来る見通しを得た。

２．モジュール状態の多様化

Nバージョンプログラムでは，作成した複数のバージョンを並列実行し，プログラムの取る状態の多様化を図る．そして，各バージョンに潜在するバグによるエラー発生のタイミングをずらし，発生したエラーを多数決により救済することにより，高信頼化を実現する．

一般に，プログラムは規模の大きなものは，複数のモジュールより構成される．Nバージョンプログラムの各バージョンが３モジュールより構成される例を図１に示す．図では，プログラムの全体仕様は，３つのモジュール仕様：A, B, Cより構成され，各

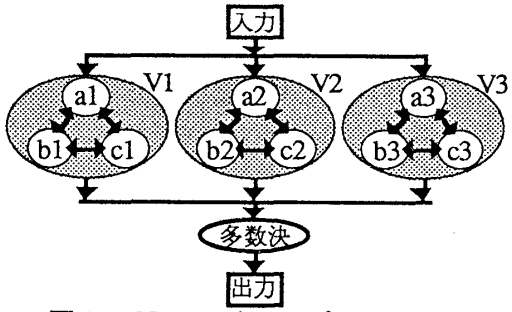

図１　Nバージョンプログラム
（バージョン数３，モジュール数３）

モジュールはそれぞれa1,a2,a3，b1,b2,b3，c1,c2,c3にて実現される．そしてバージョンV1はa1,b1,c1，V2はa2,b2,c2，V3はa3,b3,c3により構成される．

ところで図２の様に，例えばモジュールb1に対して，バージョンを構成する環境をモジュールa1とc1や，a2とc2の様にして，モジュール間インタフェースの冗長化を図る．その結果，バージョンに対して同じ入力値であっても，図の様にb1の取る状態が多様化し，バグの潜在する処理を実行する場合としない場合に別れることがある．この様にすれば，バグによるエラーを発生する場合があったとしても，多数決の原理で救済出来る可能性がある．

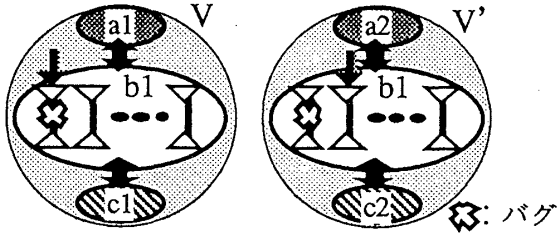

図２　モジュール状態の多様化

なお，モジュールの取る状態が異なる要因は，仕様には記述されていない部分や曖昧な部分が，プログラミングに自由度を与えることによるもので，
(1) 計算誤差，(2) 論理的には正しいが異なる値，
(3) マルチタスク処理による共有資源への相互アクセス等のタイミングのずれ，等が考えられる．

A Study of Reliability of N-Version Program diversifying Interface between Software Modules
Shoji Suzuki, Nobuyasu Kanekawa, Yoshimichi Satoh, Shin'ya Ohtsuji
Hitachi Research Laboratory, Hitachi Ltd.
7-1-1 Ohmika,Hitachi,Ibaraki 319-12,Japan

3．モジュール間インタフェースの冗長化による高信頼化の検討

図３は，図１の各バージョンを構成するモジュール同士の組み合せにより生成された27バージョンを表したものである．例えばモジュールb1に着目すると，b1を含むバージョンは，a1, a2, a3, b1, b2, b3との組み合わせであり，3×3=9個になる．即ちb1のモジュール間インタフェースの冗長度は９となる．

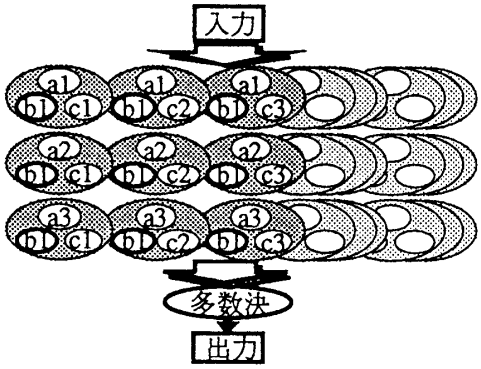

図３　モジュール組み合せによる
モジュール間インタフェースの冗長化

ここで，信頼性検討の簡略化の為に，各バージョンを構成する各モジュールの信頼度を全てｒとする．更に，モジュール状態の多様化を表す尺度として，多様化度ｓを定義する．これにより，モジュール間インタフェースの冗長化によるb1の信頼度Rmを次式にて表す：

$$Rm = (1-s)\cdot r + s\cdot Rnv(9,r) \qquad (式1)$$

但しRnv(9,r)は，多数決システムの信頼度を表す次式のモジュール数ｎ＝９の場合に相当する：

$$Rnv(n,r) = \sum_{k=0}^{[\frac{n+1}{2}]} {}_nC_k \cdot (1-r)^k \cdot r^{n-k} \qquad (式2)$$

(但し[]は整数の除算の商を表す)

(式１)は，s=0の時はb1は全く多様化されておらず，モジュール単体の信頼度ｒであることを意味する．またs=1の時はb1は完全に多様化され，b1の信頼度は９モジュールによる多数決システムの信頼度Rnv(9,r)と等価であることを意味する．他の残りのモジュールに関しても同様とする．

図３のモジュール間インタフェースの冗長化による効果は，図１内の各モジュールの信頼度を(式１)にした場合と等価になるので，図１の３モジュール構成の各バージョンの信頼度Rvは次式となる：

$$Rv = Rm^3 \qquad (式3)$$

よって，Ｎバージョンプログラム全体の信頼度RTは次式となる：

$$RT = Rnv(3, Rv) \qquad (式4)$$

以上の様にして求められたRTとｒの関係を図４に示す．図よりs=0の時は，RTは従来の３バージョンプログラムの信頼度となる．sの値が大きくなるにつれ，特にｒが0.5より大きい領域で，モジュール間インタフェースの冗長化の効果が顕著に現われており，従来より更なる高信頼化を図ることが出来る．別の見方をすれば，少ないバージョン数にて，高信頼化を得ることが出来るので，低コスト化にも有効であると言える．

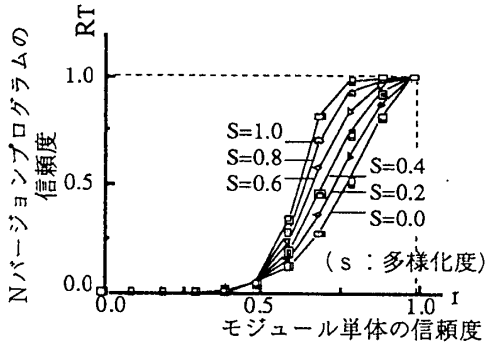

図４　Ｎバージョンプログラム
―モジュールの信頼度
（バージョン数３，モジュール数３）

4．おわりに

以上，モジュール間インタフェースの冗長化により，モジュール状態の多様化が図られる場合には，Ｎバージョンプログラムの更なる高信頼化，低コスト化に有効であることを示した．

今後の課題は，本技法のテストプログラムを用いた実験による有効性の検討と，デバッガへの適用検討である．

参考文献

[1] 当麻喜弘, 南谷崇, 藤原秀雄, "フォールトトレラントシステムの構成と設計," 槙書店, 1991

[2] A. Avizienis, "The N-Version Approach to Fault-Tolerant Systems," IEEE Trans. Software Engineering, Vol. SE-11, No.12, Dec. 1985, pp. 1491-1501