通信ソフトウェアの機能改良手法

6E－2

奥山 浩伸　森保 健治　平川 豊
NTT ソフトウェア研究所

1　はじめに

ネットワークの高機能化に伴ない、アプリケーションへの多様な要求に対する柔軟かつ迅速な対応が必要になっている。大規模ネットワークでは、多様な要求は、しばしばネットワークの一部グループにおける機能改良という形で実現される。

一方、アプリケーションの実現には、デッドロック、未定義受信などの異常動作が起らないことを保証するため、仕様検証が必要である。ところが、上記の様な一部グループにおける機能改良を実現する場合、ネットワーク全体を対象とした仕様検証をそのまま適用することはできない。例えば、ネットワークの一部グループのプロセスのみに機能改良を行なうと、新規に機能を追加したプロセスと機能を追加していないプロセスが通信を行なう場合がありうる。しかし一般に、異なった機能を持つプロセス同士の通信には、機能の相違を原因とする異常動作が起きる。

本稿では、一部グループのプロセスに対し機能追加を行なったとき、機能追加を行なったプロセスと機能追加を行なっていないプロセスの間での通信に起因する異常動作に関し、基本的な性質を明らかにする。

2　異常動作例

図1に電子掲示板サービスの仕様の一部を示す。

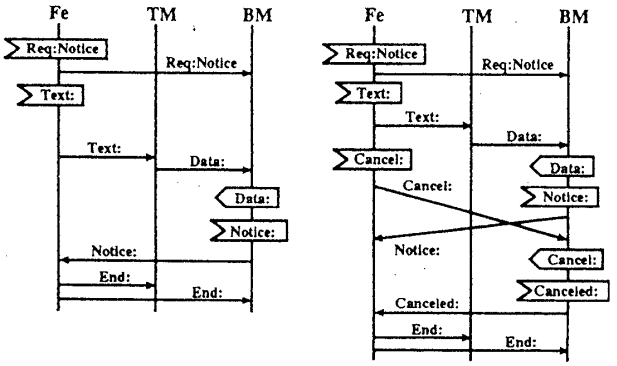

図 1: 電子掲示板サービス（既存機能）

電子掲示板サービスとは、ユーザが掲示したい内容（Text:）をフロントエンドFeに入力すると、文書整形マネジャーTMで整形データ（Data:）に変換後、掲示板マネジャーBMが掲示板に掲示する、という機能である。ただしユーザが内容を入力後に信号 Cancel: を入力すると、BMに一旦掲示された内容が消去され、その後消去の確認信号 Canceled: がFeに返送される。

（ただし掲示内容を読む機能はここでは省略している）

このサービスの運用中に、図2の仕様の新規機能を追加する場合を考える。

新規機能では Cancel: の入力が、BMにおける内容掲示に間に合えば、掲示される前の時点で掲示内容を消去することができる。ただし間に合わない場合は、既存の機能の通り、一旦掲示板に表示した後、消去される。

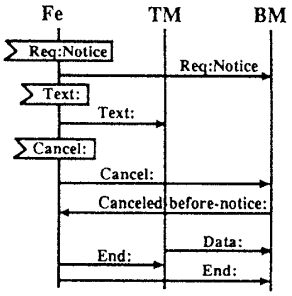

図 2: 電子掲示板サービス（新規機能）

このような機能追加を行なった仕様に対して、機能追加したグループ内での動作解析を行なうと、異常動作のないことが確認される。

しかし、機能追加を行なっていないプロセスが、機能追加したグループ内にアクセスする場合、機能の異なるプロセス間での通信となり（図3の太い矢印）、以下のような過程で異常動作が起きる。

Step1 機能追加していないプロセス Fe で、Cancel: を入力。

Step2 機能追加しているプロセス BM に Cancel: が Data: より早く着信。

Step3 BM は Fe に対し Canceled-before-notice: を送信。

Step4 機能追加していないプロセス Fe は Canceled-before-notice: を受信できない（未定義受信）。

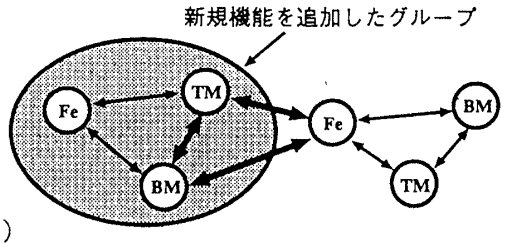

図 3: 一部グループのプロセスへの機能追加

3　異常動作に関する性質

3.1　定義と仮定

既存機能および新規機能の仕様は各々メッセージシーケンスチャート（MSC）で与えられ、ループは含まないものとする。また、プロセスは受信イベントでのみ分岐する。

A Design Method for Communications Software Evolution
Hironobu OKUYAMA Kenji MORIYASU Yutaka HIRAKAWA
NTT Software Laboratories

【定義 1】
全てのプロセスが最終状態に到達し、かつ全てのチャネルが空であるような場合以外で、動作が停止した時、これを異常動作という。
【仮定】
本稿では以下を仮定する。
(1) 既存機能の仕様は異常動作を起こさない。
(2) 機能追加したグループ内で通信を行なう場合には、異常動作は起こらない。
(3) 新規機能はネットワーク上の一部グループのみに追加される。
(4) 機能追加していないプロセスと機能追加していないプロセスが互いに通信しあう時、新規機能の外部入力イベントを実行させない。

次の 3.2 節では、以上 (1) 〜 (4) の仮定のもとで起こる異常動作に関する性質を明らかにする。

3.2 諸性質

以下では次のような記号、用語を使用する。
$-a_j^i$: プロセス i のプロセス j への信号 a 送信イベント
$+a_j^i$: プロセス i のプロセス j からの信号 a 受信イベント
既存イベント : 既存仕様に定義されているイベント
新規イベント : 既存仕様に定義されておらず、新規仕様にのみ定義されているイベント
【性質 1】
3.1 節の仮定のもとで、異常動作が起こるならば、既存イベントにより送信された信号を新規イベントが受信している。
［証明］
各プロセスは、既存イベントと新規イベントを実行し得る。全てのプロセスが既存イベントのみを実行したとすると、仮定 (1) より、異常動作は生じない。つまり新規イベントが実行されたことになるので、動作時に最初に実行される新規イベントについて考える。
最初に実行される新規イベントは分岐を構成する受信イベントである。また仮定 (4) より、最初に実行される新規イベントは内部通信信号の受信である。従って、対応する既存送信イベントが存在する。
【定義 2】
以下の条件を満たす 2 つのイベントの対 (e1,e2) をクリティカルペアとよぶ。
(2.1) イベント e1 は新規受信イベント $+a_j^i$ であり、既存イベントのみで到達できる状態 s で定義されている。
(2.2) イベント e2 は既存受信イベント $+a_j^i$ であり、状態 s から既存イベントのみで到達できる状態 t で定義されている。
(2.3) 状態 s から状態 t への全てのパス上にはプロセス j からの受信イベントはない

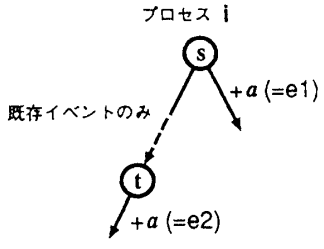

図 4: クリティカルペア

【性質 2】
3.1 節の仮定のもとで、既存イベントが送信した信号を新規イベントが受信したとする。このような新規イベントの中で最初に実行された新規イベントを e1($=+a_j^i$) とする。このとき、イベント e1 に対するクリティカルペア (e1,e2) が存在する。
［証明］
(I) イベント e1 の定義されている状態を s とすると、イベント e1 は、動作時に最初に実行された新規イベントであるので、状態 s には既存イベントのみで到達可能である。(定義 2 の条件 (2.1))
(II) まず、具体的に e2 を構成する。プロセス i の状態 s で e1= $+a_j^i$ が実行可能であり、このイベントが動作時に最初に実行された新規イベントであるから、既存機能の仕様において、i が状態 s に到達したとき、信号 a が i の j からの受信キューに存在する。既存機能からは異常動作が生ずることはないので、状態 s から既存イベントのみで到達できる状態 (これを t とおく) に既存イベント $+a_j^i$(これを e2 とおく) が存在する (定義 2 の条件 (2.2))。
(III) 同様に i の受信キューを考えると、状態 s から後に実行できるプロセス j からの最初の信号受信イベントは、信号 a の受信に限られる (定義 2 の条件 (2.3)) 。
【性質 3】
3.1 節の仮定のもとで、以下のどちらかが成立する場合、異常動作は起こらない。
(1) クリティカルペアが存在しない。
(2) クリティカルペア (e1,e2) が存在する時、新規受信イベント e1= $+a_j^i$ の定義されている MSC を用いて、対応する信号送信イベント e3= $-a_i^j$ の集合を特定する。このとき e3 の集合内に既存イベントが存在しない。
［証明］
(1) クリティカルペアが存在しない場合、性質 2 の対偶より異常動作が生ずることはない。
(2) クリティカルペアが存在するが、新規受信イベント e1= $+a_j^i$ に対応する送信イベント e3= $-a_i^j$ として既存イベントが存在しない場合、既存イベントが送出した信号を新規イベントが受信することはない。従って性質 2 の対偶より、異常動作が生ずることはない。

以上より、与えられた仕様に対し、性質 3 に関する判定を行なえば、一部グループに機能追加を行なったとき異常動作が起きるかどうかが検出できる。

4 おわりに

本稿では、ネットワーク上の一部グループで自由な機能改良を行なうために、機能の異なるプロセス間で通信が行なわれるときの異常動作の基本的性質について述べた。
今後は、ネットワークの不特定の一部グループへの機能追加を n 回繰り返すときの異常動作の性質、あるいはループを含む仕様における異常動作の性質等について検討していく。

参 考 文 献

1) M.Itoh and H.Ichikawa, “Protocol Verification Algorithm Using Reduced Reachiability Analysis” Trans. of IECE of Japan, vol.E66,No.2 pp.88-93 (1983).
2) 桧垣 博章, “分散システムにおける動的改版手法” 情報処理学会第 46 回全国大会,1P-3, pp. 195–196 (1993).
3) 桧垣 博章 他 , “システム進化支援環境 リセプティブプラットホーム” 情報処理学会第 47 回全国大会,6E-1,(1993).