概要

本研究課題では、リーダ選出アルゴリズムについて形式仕様を作成し、アルゴリズムの正当性の性質をモデル検査で検証することで、現実的な時間で検証可能なリーダ選出アルゴリズムの形式仕様の作成方法とモデル検査の実施方法を示す。

分散システムでは、システムへの負荷や故障の観点から、集中管理は好ましくなく、同じ役割を持つ複数のプロセスでシステムを設計する方がよいとされてる。しかし、データの整合性担保などは選任のプロセスがいた方が、処理が容易になる。

分散システムを構成する複数のプロセスの中から、1つの選任プロセス、つまり「リーダ」を選ぶ処理をリーダ選出という。リーダ選出のアルゴリズムとしては、これまでに、様々なアルゴリズムが提案されている。

近年は分散データベースやシステムの耐障害性の組み込みなどでリーダ選出が利用されているため、リーダ選出アルゴリズムの正確性はシステム運用の視点からも非常に重要になっている。そのため、リーダ選出アルゴリズムをモデル化し、モデル検査ツールを利用して、そのようなアルゴリズムが所望の性質を満たしていることを検証されることが増えてきた。しかしながら、モデル化の難しさや、状態爆発による非現実的な検証時間の長さが問題になっている。

本稿の実験ではブリーアルゴリズム、Chang-Roberts アルゴリズム、Franklin アルゴリズムの 3 つのリーダ選出アルゴリズムについて Maude にて形式仕様を作成した。また、作成した形式仕様を基に、リーダ選出アルゴリズムの正当性の性質や各アルゴリズムが、保証すべき性質が満たされているかの確認をモデル検査で検証した。

ブリーアルゴリズムでは、あるプロセスがリーダの停止を検出すると次の選任処理を開始する。選任を開始したプロセスは、自身の ID より大きな ID をもつすべてのプロセスにメッセージを送信する。メッセージを送ったプロセスから返信がない場合は、選任のプロセスがリーダになる。反対に、選任のプロセスより大きな ID をもつプロセスから返信があった場合は、選任を交代する。最終的には、返信するプロセスがなくなり、残った 1 つのプロセスがリーダになる。本稿では、上述の動作をするブリーアルゴリズムを、8 つの観測可能成分で状態遷移システムとして形式化し、11 の書き換え規則で形式仕様として表現した。また、作成した形式仕様を用いて満たすべき性質の確認をモデル検査で検証した。検証の実験では、ブリーアルゴリズムの対象となるプロセス数を 5 つにして、モデル検査を行った。検証実験の結果、ブリーアルゴリズムは、リーダ選出アルゴリズムとしての性質が満たされていることを確認できた。

ブリーアルゴリズムでは、すべてのプロセスが、同期的にタイミングを合わせて 1 ステップずつ選任処理を進める。そのため、本来、非同期で処理を実施する Maude ではモデル検査を行うことが難しい。だが、本稿では作成した形式仕様の書き換え規則に、3 つの同期的な対応を行うことで、ブリーアルゴリズムのモデル検査を行うことにした。対応の結果、リーダ選出アルゴリズムとしての性質を満

たしていることが確認できたため、対応には効果があったと考える。

Chang-Roberts アルゴリズムは、非候補者のプロセスが、リーダの不在を検知すると選任処理を開始する。リーダの不在を検知したプロセスは、始動プロセスとして候補者となり、隣のプロセスに自身のプロセス ID を含むメッセージを送る。メッセージを受け取ったプロセスが非候補者の場合は、メッセージをそのまま隣のプロセスに中継し、メッセージを受け取ったプロセスが候補者の場合は、自身のプロセス ID と受信したメッセージのプロセス ID を比較する。自身のプロセス ID の方が大きい場合は、受け取ったメッセージを隣に送る。反対に、自身のプロセス ID の方が小さい場合は、受け取ったメッセージを破棄する。この処理を最小のプロセス ID を含むメッセージだけがリングを一周するまで行う。本稿では、上述の動作をする Chang-Roberts アルゴリズムを、4 つの観測可能成分で状態遷移システムとして形式化し、9 の書き換え規則で形式仕様として表現した。アルゴリズムが満たすべき 5 つの性質は、LTL 式で記述している。また、作成した形式仕様を用いて満たすべき性質の確認をモデル検査で検証した。検証の実験では、Chang-Roberts アルゴリズムの対象となるプロセス数を 5 つにし、並び順を考慮した初期状態を 2 つ定義して、モデル検査を行った。検証実験の結果、Chang-Roberts アルゴリズムは、リング状に配置されたプロセスの並び順に関係なく、リーダ選出アルゴリズムとしての正当性の性質が満たされていることを確認できた。また、Chang-Roberts アルゴリズム固有の 3 つの性質についても満たされていることが確認できた。

Franklin アルゴリズムは、非イニシエーターのプロセスが、リーダの不在を検知すると選任処理を開始する。リーダの不在を検知したプロセスは、イニシエーターとなり、両隣のプロセスに自身のプロセス ID を含むメッセージを送る。メッセージを受け取ったプロセスが非イニシエーターの場合は、パッシブプロセスとしてメッセージをそのまま隣のプロセスに中継するが、メッセージを受け取ったプロセスがイニシエーターの場合は、両隣のプロセスから受信したメッセージのプロセス ID のうち、大きな方のプロセス ID と自身のプロセス ID を比較する。自身のプロセス ID の方が大きい場合は、再度、両隣のプロセスに自身のプロセス ID を含むメッセージを送る。自身のプロセス ID の方が小さい場合は、パッシブプロセスとなる。自身のプロセス ID と等しい場合はリーダとなる。本稿では、上述の動作をする Franklin アルゴリズムを、4 つの観測可能成分で状態遷移システムとして形式化し、12 の書き換え規則で形式仕様として表現した。アルゴリズムが満たすべき 2 つの性質は、LTL 式で記述している。また、作成した形式仕様を用いて満たすべき性質の確認をモデル検査で検証した。検証の実験では、Franklin アルゴリズムの対象となるプロセス数を 5 つにし、並び順を考慮した初期状態を 2 つ定義して、モデル検査を行った。検証実験の結果、Franklin アルゴリズムは、リング状に配置されたプロセスの並び順に関係なく、リーダ選出アルゴリズムとしての正当性の性質が満たされていることを確認できた。

キーワード： モデル検査、分散アルゴリズム、リーダ選出、Maude、安全性、

活性、状態遷移システム