

氏名	モハメド ファルク ナズリーン バヌ MOHAMED FAROOK NAZREEN BANU
学位の種類	博士（工学）
学位記番号	博第822号
学位授与の日付	平成24年3月23日
学位授与の条件	学位規則第4条第1項該当 課程博士
学位論文題目	A Study on Efficient Consensus Algorithms for Byzantine-Prone Distributed Systems (ビザンチン故障下の分散システムにおける効率的な合意アルゴリズムに関する研究)
論文審査委員	主査 教授 和田 幸一 教授 和田山 正 准教授 片山 喜章

論文内容の要旨

分散合意問題は、耐故障分散システム設計における重要な基礎問題の一つである。n 台の計算機（プロセス）からなる分散システムにおいて、各プロセスがそれぞれある値（提案値）を保持している状況を考える。分散合意問題は、全プロセスの保持する値をあるプロセスの提案値に合意させる問題として定義される。同問題はアトミックブロードキャスト、グループメンバシップ等、多くの応用を持つ。合意問題は一般に故障の存在する分散システムを対象として考えられる。対象としている故障モデルの種別（停止故障あるいはビザンチン故障）、および非同期、同期の区別により、分散システムのモデルにはいくつかのバリエーションがあるが、そのいずれにおいても、これまでに多くの分散合意問題に関連した研究が行われている。本論文では、非同期および同期システムの両方に対して、ビザンチン故障下における分散合意問題（ビザンチン合意問題）を対象とした研究を行った。ビザンチン故障とは、故障プロセスが任意の動作（アルゴリズムに従わない動作も含む）を認める、最も困難な故障モデルの一つである。

本研究における非同期システム上での成果を以下に述べる。非同期システムにおいて、本研究では 1 通信ステップ合意可能なビザンチン合意アルゴリズムについて研究を行った。一般には、ビザンチン合意問題を解く任意のアルゴリズムに対しては、最悪時ステップ数が 2 以上となること、および、最良時に 1 ステップを実現する場合、最悪時ステップ数が 3 以上となることが既知の結果として知られている。本研究は、この不可能性を回避する新しいアルゴリズム DEX を提案する。アルゴリズム DEX は、入力の困難さに応じて求解時間が変化するという特徴を有するアルゴリズムであり、容易な入力（例えば、全プロセスの提案値がすべて同じである等）において、1 ステップ合意を達成することが保証されている。このような特徴はいくつかの既存アルゴリズムにおいても示されているが、アルゴリズム DEX は、さらに適応性、および二重加速性という 2 つの特徴を有している。適応性は、1 ステップ合意の達成が保証される入力の集合が、実故障プロセス数に応じて決定されるという特徴である。また、二重加速性は、1 ステップ合意が達成されなかった場合においても、そのような入力の一部に対して、2 ステップ合意を達成することを保証するという特徴である。二重加速性は本研究において初めて提案された概念であり、アルゴリズム DEX は、1 ステップ合意および 2 ステップ合意の両方を（部分的な入力集合に対して）実現する初めてのアルゴリズムである。

同期システムについての成果を以下に述べる。同期システムにおいて、本研究では、ビザンチン故障モデルをさらに発展させた、モバイルビザンチン故障というモデルに対する合意問題の可解性に関して研究を行った。モバイルビザンチン故障は、各時刻における故障数の上限が定義されているが、故障プロセスの集合（すなわち、どのプロセスが故障しているか）は時間の経過とともに変化するモデルである。既存の結果として、Garay らが、モバイル故障モデルにおいて故障数が全プロセス数の 6 分の 1 を越える場合において、ビザンチン合意が可解であることを示している。一方で、6 分の 1 以上のプロセスが同時に故障可能な状況でビザンチン合意問題を解くアルゴリズムが構成可能であるかどうかは未解決問題であった。本研究では、この問題に対する部分的な解を与える。具体的には、故障プロセス数の比率が 4 分の 1 以上であっても正しくビザンチン合意問題を解くアルゴリズムを示す。

論文審査結果の要旨

分散合意問題は、耐故障分散システム設計における重要な基礎問題の一つである。n台の計算機（プロセス）からなる分散システムにおいて、各プロセスがそれぞれある値（提案値）を保持している状態を考える。分散合意問題は、全プロセスの保持する値をあるプロセスの提案値に合意させる問題として定義される。同問題はアトミックブロードキャスト、グループメンバシップ等、多くの応用を持つ。合意問題は一般に故障の存在する分散システムを対象として考えられる。対象としている故障モデルの種別（停止故障あるいはビザンチン故障）、および非同期、同期の区別により、分散システムのモデルにはいくつかのバリエーションがあるが、そのいずれにおいても、これまでに多くの分散合意問題に関連した研究が行われている。本論文では、非同期および同期システムの両方に対して、ビザンチン故障下における分散合意問題（ビザンチン合意問題）を対象とした研究を行った。ビザンチン故障とは、故障プロセスが任意の動作（アルゴリズムに従わない動作も含む）を認める、最も困難な故障モデルの一つである。

本研究における非同期システム上での成果を以下に述べる。非同期システムにおいて、本研究では1通信ステップ合意可能なビザンチン合意アルゴリズムについて研究を行った。一般には、ビザンチン合意問題を解く任意のアルゴリズムに対しては、最悪時ステップ数が2以上となること、および、最良時に1ステップを実現する場合、最悪時ステップ数が3以上となることが既知の結果として知られている。本研究は、この不可能性を回避する新しいアルゴリズムDEXを提案する。アルゴリズムDEXは、入力の困難さに応じて求解時間が変化するという特徴を有するアルゴリズムであり、容易な入力（例えば、全プロセスの提案値がすべて同じである等）において、1ステップ合意を達成することが保証されている。このような特徴はいくつかの既存アルゴリズムにおいても示されているが、アルゴリズムDEXは、さらに適応性、および二重加速性という2つの特徴を有している。適応性は、1ステップ合意の達成が保証される入力の集合が、実故障プロセス数に応じて決定されるという特徴である。また、二重加速性は、1ステップ合意が達成されなかった場合においても、そのような入力の一部に対して、2ステップ合意を達成することを保証するという特徴である。二重加速性は本研究において初めて提案された概念であり、アルゴリズムDEXは、1ステップ合意および2ステップ合意の両方を（部分的な入力集合に対して）実現する初めてのアルゴリズムである。

同期システムについての成果を以下に述べる。同期システムにおいて、本研究では、ビザンチン故障モデルをさらに発展させた、モバイルビザンチン故障というモデルに対する合意問題の可解性に関して研究を行った。モバイルビザンチン故障は、各時刻における故障数の上限が定義されているが、故障プロセスの集合（すなわち、どのプロセスが故障しているか）は時間の経過とともに変化するモデルである。既存の結果として、Garayらが、モバイル故障モデルにおいて故障数が全プロセス数の6分の1を越える場合において、ビザンチン合意が可解であることを示している。一方で、6分の1以上のプロセスが同時に故障可能な状況でビザンチン合意問題を解くアルゴリズムが構成可能であるかどうかは未解決問題であった。本研究では、この問題に対する部分的な解を与える。具体的には、故障プロセス数の比率が4分の1以上であっても正しくビザンチン合意問題を解くアルゴリズムを示す。