分散量子計算プラットフォーム
-量子インターネットで繋がった量子コンピュータの計算力相互融通-

1. 背景

将来世界を変えるエラー訂正付き量子コンピュータは、ハードウェアの完成後も、実行における課題がある。素因数分解などのいわゆる高速な量子アルゴリズムを実行するには大量の T ゲートが必要であり、エラー訂正付き量子コンピュータで T ゲートを実行するには、T ゲートを実行する際に消費するリソース量子状態 |A>をまず生成しなければならない。|A>の生成自体も大きな量子計算処理であるため、目的の量子アルゴリズムの実行に必要な数の |A>の確保は、エラー訂正付き量子計算を実現する上での課題となっている。計算内容に依存するが、量子コンピュータの処理のうち半分以上が |A>の生成になると見込まれる。

量子コンピュータの研究開発が進む一方で、量子インターネットの研究開発も進んでいる。量子インターネットは任意の 2 地点 間で量子もつれ対を生成する通信インフラでる。量子インターネットで生成した量子もつれ対を利用して量子テレポーテーションを実行すると任意の 2 地点間で任意の量子状態を送受信する事ができ、遠距離での分散量子計算が可能となる。量子インターネットが運ぶものは量子情報であり、古典インターネットとは機能的に異なる。

2. 目的

本プロジェクトでは、エラー訂正が実装された量子コンピュータと量子インターネットが存在する状況を想定して、量子インターネットを介して世界中の量子コンピュータから |A>を集めてくる相互扶助のシステムを提案・開発する。これにより、各ユーザが量子計算力を相互融通して、各々の量子コンピュータでは実行できないサイズの量子計算を実行できるようにする。

3. ソフトウェア開発内容

（今回開発したソフトウェアで解決する課題、動作環境、構成、機能等を、図等を使用して記述）

本プラットフォームは、ハイブリッド P2P の形態を取る（図 1）。中央サーバは古典コンピュータであり、クライアントである量子コンピュータ群の情報を管理している。各クライアントは、古典通信と量子通信の双方を実行できる量子コンピュータである。あるクライアント（オーナー） から発された分散計算リクエストはサーバで処理され、他のクライアント （コラボレーター） をオーナーに紹介する。オーナーとコラボレーターは直接量子通信し、|A> をコラボレーターからオーナーに提供する。

本プロジェクトでは、エラー訂正付き量子コンピュータと量子インターネットの存在を想定する。また、量子コンピュータのライブラリもしくは OS が T ゲートの実行と |A>の生成を管理していることを想定し、この部分に、本プラットフォームで |A>を供給することを想定する。現状、量子コンピュータのライブラリは Python がもっとも一般的であるため、本プロジェクトも Python で実装した。

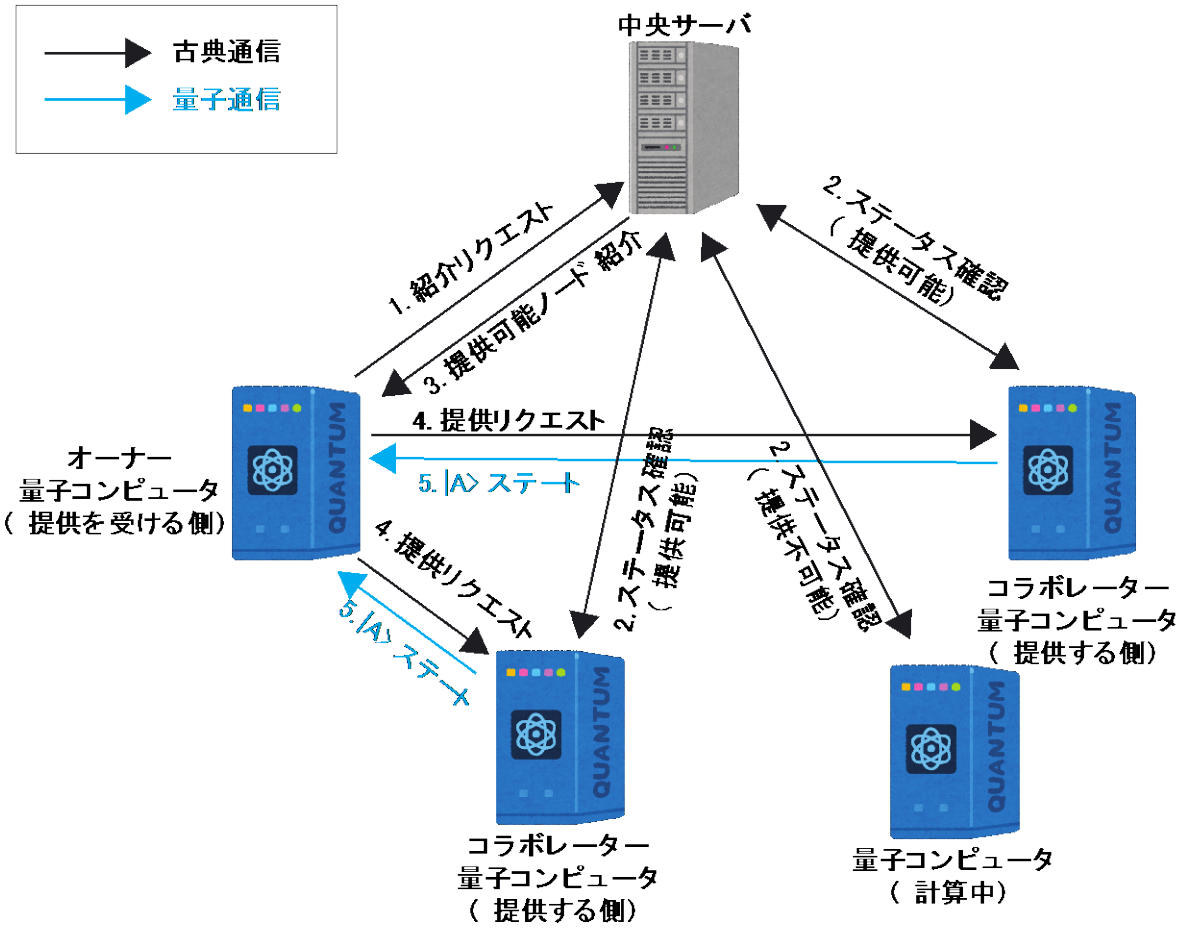

図 1 分散量子計算開始シーケンス

本プロジェクトで開発したソフトウェアの機能を以下にまとめる。

- 中央サーバ
  - ノード登録機能
  - ノード管理機能
  - 認証局機能
  - ジョブ管理機能
  - データベース機能
  - 可視化機能
- クライアント
  - 中央サーバ登録機能
  - 認証局クライアント機能
  - |A>供給リクエスト機能（オーナー機能）
  - |A>供給機能（クライアント機能）
  - 量子通信機能（シミュレーション）
- プラットフォーム全体機能

- 中央サーバ-ノード間通信機能
- ノード間通信機能

古典通信部分の暗号化や認証については、耐量子暗号対応の標準化が進んでいるプロトコルを選択するなど、量子コンピュータに解読されないよう配慮した。

4. 新規性・優位性

（今回開発したソフトウェアの新規性、類似のものと比較した場合の優位性等を記述）

量子コンピュータにおける分散計算は、理論提案やアーキテクチャの研究にとどまり、ユーザを想定したシステムやプラットフォームの提案はおこなわれてこなかった点で、まず本プロジェクトに新規性がある。

本プロジェクトで提案する分散量子計算では、リソース量子状態|A>の作成にのみ分散計算を利用してコラボレーターノードに計算能力を融通してもらい、量子データの保持と量子回路の実行はオーナーノードで実施する。この仕組みは、量子回路の実行を分散しておこなう既存提案に対して以下の pros/cons がある。

- Pros:
  - owner が量子データを全て保持しており、コラボレーターが突然シャットダウンするなどしても量子データが失われないため、コラボレーターの異常に対して耐性がある（量子データはコピーできないため、コラボレーターに量子データを預けて量子回路を実行してもらう手法には、コラボレーター量子コンピュータの信頼性などのリスクが有る）
  - 実行する量子回路についての情報をコラボレーターに秘匿できる（量子アルゴリズムについての情報を全く流出させずに他ノードの計算力を利用できる）
- Cons: 量子通信リソースを大量に消費する

現行コンピュータの分散計算の場合、分散並列しても、原理的に計算能力が上昇するわけではない（例えば、1CPU×100 時間と 100CPU×1 時間は同じ 100CPU 時間である）。一方量子コンピュータの場合、並列化して多くの量子ビットを用いると、量子もつれと重ね合わせによって、より大きな状態空間を扱えるようになる。すなわち、1 量子 CPU×100 時間より、100 量子 CPU 時間のほうがエンタングルメントと重ね合わせでより大きな空間を扱って計算できる。量子計算では古典計算よりも、分散計算で計算資源を相互融通するメリットが大きいと考えられる。

また、エラー訂正付き量子計算のワークロード管理に|A> の生成量・消費量を用いている点に新規性がある。量子アルゴリズムの実行には|A>の生成がボトルネックとなる。したがって、量子コンピュータの計算能力の評価指標として、|A>の生成能力である Akeps (Aket Per Second) を提案する。

5. 期待されるユーザー価値と社会へのインパクト

（今回開発したソフトウェアをユーザーが利用することによって得られる価値、及び、利用が拡大することで活

性化される産業分野・技術分野等の範囲やその効果を可能な限り具体的、定量的に記載）

エラー訂正付き量子コンピュータや量子インターネットが実現した将来、小さな量子コンピュータのユーザが集まって大きな量子計算能力を持ち、皆で共有して利用することができる。エラー訂正付き量子コンピュータが実現したら、大規模で計算力の高い量子コンピュータによる革新的な発見や高速情報処理が社会や人類の発展を牽引すると見込まれる。このとき、資金で優位に立てる一部の大企業や研究機関が常に最大の量子コンピュータを有して優位に立ち続け、それ以外の企業・研究機関は比較的中小規模の量子コンピュータしか利用できず、量子前提時代における競争優位性を失う状況が想定される。インターネットを介した分散計算でスーパーコンピュータに比する計算能力を実現できることは古典コンピュータにおいて明らかであり、これを量子コンピュータにおいても実現できれば、大規模な量子コンピュータを有しないもしくはアクセスできない企業・研究機関でも、利活用において研究・事業を加速することが可能となる。すなわち、量子情報革命の機会を平等に提供することに貢献する。

6. 氏名（所属）

永山翔太（株式会社メルカリ）、中島博敬（株式会社メルカリ）