様式３

論　文　内　容　の　要　旨

氏　　名	（　竹内 勇貴　）
論文題名	Verification methods for quantum computing: from subuniversal to universal （非万能・万能量子計算の検証）

論文内容の要旨

万能量子コンピュータは任意の量子系の時間発展をシミュレート出来るという意味で万能であり、古典コンピュータにとって困難な問題のいくつかを効率良く解くことが出来る。特に、サンプリング問題を考えることで古典計算に対する優位性を実証することも出来る。しかし、万能量子コンピュータはその万能さ故に実現が難しい。そこで、近年、比較的実現が容易な非万能量子コンピュータが注目を浴びている。非万能量子コンピュータは応用が限定されているが、古典計算に対する優位性を実証するという目的においては十分であるということが分かっている。両者の実現に共通する要求として計算結果が正しいかどうかを効率良く確認出来ることが挙げられる。このような操作は検証と呼ばれており、検証者に要求される操作が単一量子ビットに対する操作のみである、多項式時間で動作する、量子状態が従う確率分布を仮定しないなどの条件を満たしていることが望ましい。検証プロトコルはいくつかの種類に分けることが出来、本論文ではその内の重要な二種類に注目する。

一つ目は、あるテストをパスした元で正しくない結果を得ている確率の上限を求めるという方法である。この方法は、ブラインド量子計算を利用することで実現出来る。ブラインド量子計算は、量子コンピュータを持たないクライアントが、計算内容を漏洩することなく量子コンピュータを所持しているサーバに計算を委託することを可能にするプロトコルである。しかし、先行研究では、二者間の量子通信路などが理想的であると仮定しており、実際に雑音がある状況では計算の委託が成功する確率が指数関数的に下がってしまうという問題点がある。

二つ目は、測定型量子計算のために用意した量子状態が理想的な状態にどれだけ近いか(忠実度)を推定する方法である。忠実度が高ければ、その状態を測定して得られる確率分布も近いと言えるため、このような操作も検証である。しかし、任意の量子状態を効率良く検証することは量子コンピュータをもってしても難しいということが計算量的な観点から分かっているため、どのような量子状態ならば検証可能であるかは重要な問題である。また、特別な場合を除いて必要な測定回数が(量子状態を構成する量子ビットの数の多項式ではあるが)多いという問題点もある。

本論文では、上記の問題を解決するための研究を行った。一つ目に関しては、既存のプロトコルに雑音耐性を付与した。また、二つ目の方法に関しては、既存の方法では検証出来なかった量子状態も検証可能であることを示し、検証可能であることが分かっていた状態に関しては測定回数を減らし効率化を行った。これらのプロトコルは上記で述べた検証プロトコルに望まれる三つの条件を満たしている。これらに加えて、既存の非万能量子計算モデルにさらに制限をかけることで、既存のプロトコルで検証可能な計算モデルの提案も行った。本論文の研究成果は、量子計算の検証だけではなくクラウド量子計算や非万能コンピュータの実現にもつながる成果であると考えられる。

様式７

論文審査の結果の要旨及び担当者

氏　名　（　竹内勇貴　）		
	（職）	氏　名
論文審査担当者	主査　教授	井元　信之
	副査　教授	鈴木　義茂
	副査　教授	北川　勝浩

論文審査の結果の要旨

昨今IBMをはじめとする小規模量子コンピューターや量子シミュレーターの試験的クラウドサービスが国内外で始まっている。クラウドは京などのスーパーコンピューターと同じく、自前では所有できないユーザーにとって欠かせないサービスである。このときの問題点は、(1)本当に量子コンピューターなのか？（これは買ってきた量子コンピューターが目の前にあっても同じ）(2)ユーザーである自分が何をしたいかを量子コンピューター側に悟られずに仕事だけしてもらえるか?を検証することである。この問題は実用上の意義にとどまらず、どういう条件のもとでどこまで検証が可能かを明らかにするという点で理学理論の範疇と認識されている。たとえば(1)では検証したいユーザーの能力を古典的手段に限定することが望ましいが、多少量子技術を持っているとして条件を緩和することが考えられ、また検証したい対象が汎用量子コンピューターなのか特殊用途の量子コンピューターなのかによって違うことが予想される。(2)は一般にブラインド型計算と呼ばれ、古典情報理論の方法は前からあるがそれは量子コンピューターには使えない検証法であり、必要なのはブラインド型量子計算である。また(1)(2)に共通する問題として、(3)クラウド通信に量子通信を用いるときに、これまでは伝送路に雑音がない場合ばかり考えられて来たが、現実には雑音があるので、その場合どこまで検証可能かを扱う理論はなかった。

竹内勇貴氏の博士論文は以上の課題に果敢に切り込んだものである。先行研究を詳細に調査した上での信頼できる理論構築を行ったものであるが、先行研究にない独創性として、「エラー耐性のあるブラインド量子計算プロトコル」を提案したことが大きな特徴である。より詳しく言うと、「ノイズレベルが、CSS符号（これは既存の量子エラー訂正符号）が耐えられるレベル以下の場合、または集団ノイズ（たとえば光伝送路の屈折率や複屈折率の揺らぎは光子群の通過時間に比べて遅いので、それぞれの光子は独立なノイズを受けるのでなく集団が同じノイズを受ける）の場合には、エラーの影響を除くことができる。この方法はuniversal（汎用）量子コンピューターの検証に使える」ことを示した。他にも関連する結果として「ハイパーグラフ状態（これは最近の新しい量子コンピューティングに使われる量子状態）のフィデリティ（目的とする状態にどのくらい近いかを％で数値化したもの）を推定する方法」を提案した。これは量子コンピューターの検証に欠かせない方法である。また従前より（ハイパーを冠しない）グラフ状態のフィデリティ推定法はあったが、それを大きく効率化した方法を提案した。これらの研究の過程でもう一つ独創性を挙げるならば、汎用量子コンピューターに話を限るのでなく、「subuniversal（特殊用途）の量子計算」も検討して、その検証に必要なユーザーの能力を緩和する方向に理論を進化させたことが挙げられる。

以上のように竹内氏の博士論文は上記三課題(1)(2)(3)の解決に向けて実質的で重要な一歩を踏み出したものであり、極めて有用性が高いばかりでなく、状況を限定した場合に条件がどれだけ緩和されるかという理論も押し進めた研究といえる。よって博士（理学）の学位論文として価値のあるものと認める。