様式 C-19

科学研究費補助金研究成果報告書

平成 22 年　1 月　　29 日現在

研究種目：若手研究(B)
研究期間：2007 年度～　2009 年度
課題番号：19700019
研究課題名（和文）　分散環境における量子計算量能力のネットワーク形状に着目した解析
研究課題名（英文）　Analysis of Quantum Computational Power on Distributed Environments of Various Network Topologies

研究代表者
谷 誠一郎　(SEIICHIRO TANI)
日本電信電話株式会社ＮＴＴコミュニケーション科学基礎研究所
協創情報研究部　主任研究員
研究者番号：70396183

研究成果の概要（和文）：
量子計算能力を持つ通信ノードを量子通信路によって相互に接続することにより構成される量子ネットワーク上において，分散している入力に依存する関数計算（分散計算）を行うために要する量子通信量を検討した．その結果，分散計算に要する量子通信量は，計算すべき関数とネットワークの形状を規定するパラメータで特徴づけられることを明らかにした．さらに，具体的な問題に対して，本結果を応用することにより，準最適な量子通信量が得られた．

研究成果の概要（英文）：
This study considered distributed computing on quantum networks, in which quantum communication and computation are available, of various topologies. It was proved that the amount of communication required to perform distributed computing on the quantum networks can be characterized with some parameters associated with their topologies as well as the function to be computed. As an application, we obtained sub-optimal amounts of communication required to solve certain distributed computing problems.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
19 年度	1,200,000	0	1,200,000
20 年度	1,100,000	330,000	1,430,000
21 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,200,000	600,000	3,800,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：アルゴリズム理論，量子分散計算

１．研究開始当初の背景

将来の情報処理技術として，1990 年以前から量子通信・量子暗号を中心に，量子情報処理が盛んに研究されてきた．特に 1994 年に P. Shor が古典的計算手法では困難とされる因数分解のための効率的な量子アルゴリズムを発見して以来，量子計算の可能性が急速

に注目されるようになり，量子通信・量子暗号とともに一大研究分野となった．やがて量子通信と量子計算の融合分野（量子分散計算）が生まれ，最も重要な研究分野の一つとして認識されるに至った．量子分散計算の研究は主に２つあるいは３つのノードで構成されるネットワークや，任意のノードが互いに結合している完全グラフ型ネットワークを想定したものであった．これに対して，本課題の研究代表者は，分散計算分野の代表的な問題である「リーダ選挙問題」が，任意の形状の匿名量子ネットワーク上で可解であることを示し，古典分散計算との計算可能性の違いについて明らかにした．しかしながら，匿名でなくかつ多様な形状の現実的なネットワークにおいて，量子分散計算は，古典分散計算に比べて，どの程度優位性があるのかほとんど明らかになっていなかった．

２．研究の目的

多くノードから構成される様々な形状のネットワークで量子分散計算の計算限界を明らかにする．具体的には，

（１） どのような計算タスクが，
（２） どのようなネットワーク形状に対して，
（３） どの程度の量子通信量で実行可能なのか

ということを明らかにすることにより，量子分散プロトコル設計の指針を与える．

３．研究の方法

多数のノードから構成される量子通信可能なネットワーク上の2つのノードに入力ビット列が分散して与えられている時に、その入力に依存する論理関数を計算するのに必要な量子通信量を，ネットワークの形状を示すパラメータと，論理関数の種類により，定量的に解析する．

４．研究成果

(1)

上図は，ノードＡおよびＢがネットワークに接続している様子を模式的に示したものである．ＡおよびＢが入力ビット列 x および y を与えられたときに，論理関数 f(x,y) を計算することが目的となる．

十分小さな誤り率を許す場合、必要な量子通信量の下界は、上記2つのノードが直結しているときに必要な量子通信量および、ネットワークの形状を規定する数種のパラメータで特徴づけられることを明らかにした。 より具体的には，以下の通りである．

- 二つのノードＡとＢにそれぞれ n ビットの入力 x,y が与えられるものとする．
- ＡとＢが接続するネットワークG上においてＡＢ間の最短パスの長さをsとする．
- ＡとＢが量子通信路で直結している場合に関数fを計算するために必要な量子通信量をQ(f)とする．

このとき，ネットワークＧ上でＡとＢがfを計算するために要する量子通信量は，少なくとも，

$$C \ s \ (Q(f) - \log n) / \log w$$

であることを明らかにした．ここで，Ｃは定数であり，w はＧをグラフとみたときの密度（枝の数）に関係するパラメータである．例えば，リング状のネットワークであれば，w は定数となる．
上記の結果からわかることの一例を以下に述べる．Q(f)が log n よりも真に大きい場合，wが定数であるようなネットワーク上では，ＡとＢが直結している場合のプロトコルをネットワークＧの最短経路上でシミュレートして得られるプロトコルが，最適なプロトコルであるということを示している．つまり，この場合，ＡとＢが直結している単純な場合で最適なプロトコルを設計すればよいことになる．
上記の結果を得るにあたり，重要なアイデアは，ＡとＢがランダムなビットストリングを予め共有していることを許すモデルを導入したことにある（下図）．そのようなモデルは，現実の状況下においては，明らかに不自然であるため，仮想的なモデルにすぎないが，証明を完成させるために重要な役割を果たしている（上記の仮想モデルは，証明の途中で出現するだけであり，成果自体は，ランダムビットを共有していることは仮定していない）．

ランダムなビット列

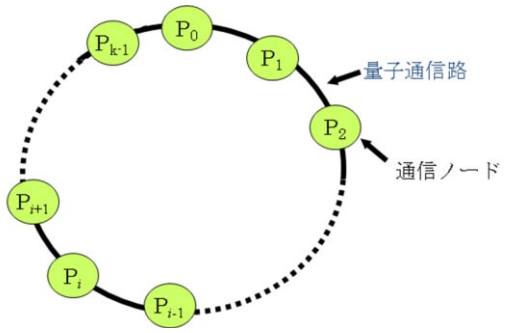
さらに本研究では，ネットワークＧ上でＡとＢがfを計算するために要する量子通信量の下界は，

$$C \ s \ (Q(f) - \log s) / \log w$$

であることも明らかにした．これは，nよりもsが小さいとき，よりよい下界を与える．
また，アプリケーションによっては，出力が誤ることは許容できないが，通信量や計算量は平均として少なければよいという場合がある．このような問題設定に対しても，関数を計算するための平均量子通信量の下界値を，入力が与えられる2つのノードが直結しているときに必要な平均量子通信量および、ネットワークの形状を規定するパラメータで同様に特徴づけられることを明らかにした．

上記の定理は、2つのノードに入力が与えられることを仮定しているが、さらに多くのノードに入力が分散して与えられる、より一般的な設定にも適用可能な場合がある。そのような場合の典型例として、リング型ネットワークにおいて，各ノードの優先順位に重複がないか検査する問題をとりあげた．具体的には次ように定義される問題をリング型ネットワーク上で検討した．

[問題 DISTINCTNESS] k個のノードからなるネットワーク上の各ノードは，入力として，0からL-1までの範囲内にある一つの整数を与えられる(ただし，L>=k)．このとき，同じ数を入力として持つノードのペアが存在するかどうか判定せよ．



上記の問題を解くために要する量子通信量を以下のようなアイデアにより求めた．すなわち，問題DISTINCTNESSをリングネットワーク上で解くプロトコルがあった場合，2ノードAおよびBに分散して与えられた入力ビット列に対して，ある種の関数f(x,y) を解くことに用いることができることを示した．これにより，前述の定理を適用し，DISTINCTを解くのに要する量子通信量は次の下界をもつことを明らかにした．

$$C\ k\ (k^{1/2}+\log\log L) \qquad C:\text{定数}$$

さらに，問題 DISTINCTNESS を解くアルゴリズムを考案し，その量子通信量が以下であることを証明した．

$$C'\ k\ (k^{1/2}\ \log k\ +\log\log L) \qquad C':\text{定数}$$

上記の上界と下界はほとんど一致しており，準最適な量子通信量であると結論づけられる．

また，本問題の一般化として，次のような問題が考えられる．

[問題 MAXCOALITION] k 個のノードからなるネットワーク上の各ノードは，入力として，0 から L-1 までの範囲内にある一つの整数を与えられる(ただし，L>=k)．このとき，同じ入力をもつノード同士を一つのグループと考えると，最大のグループのサイズ（ノード数）を求めよ．

上記問題を解いた結果，出力が 1 か 2 以上かにより，DISTINCTNESS を解くことができるため，DISTINCTNESS の下界はそのまま成立する．一方，上界は，そのままでは成り立たないが，同じ上界を持つ別のアルゴリズムが構成できる．

上記結果は，分散した入力に対する関数計算問題を解くために必要な量子通信量が，ネットワークの形状にどのように依存するかを示したものであるが，この種の成果は，これまでほとんど得られていなかった．現実のネットワークが複雑な形状をしていることを考えれば，様々な形状のネットワーク上での量子計算は，実用的にも重要な課題と考えられる．本課題の成果の一つとして，具体的な問題をリング上で解いた場合の準最適な量子通信量を求めることができた．今後は，ネットワークの枝数が多い場合に，（準）最適な量子通信量をいかにして得るかということが課題となる．場合によっては，量子通信量の下界を与える評価式をより厳密にしていくことが必要と考えられる．

(2) 上述の成果は，一般的なネットワークにおける量子通信量の下界を与える枠組みを提供するものであり，これに個々の関数に依存した情報を組み合わせることにより，具体的な通信量の下界が得られる．このため，通信量と深い関連を持つ質問計算量の観点から，様々な論理関数の複雑さを検討した．具体的には，論理関数の集合を，関数値を真にする割り当ての数によりグループわけを行い，グループごとに質問計算量の解析を行った．

まず，一般性を失うことなく，論理関数は N 変数のものだけを考える．入力は，この N 変数に対する真偽の割り当てであり，長さ N のビット列と見ることができる．質問計算量で用いるオラクル計算モデルでは，入力の N ビ

ット

$$x[1],\ldots,x[N]$$

がオラクルというブラックボックスとして与えられ，アルゴリズムが入力にアクセスするためには，オラクルに対して，「i ビット目は何か？」 という質問をしなければならない．オラクルは，この質問に対して，x[i]を答えとして返す．
質問計算量におけるコストとは，（論理関数の値を確定するまでに要する）質問回数である．量子質問計算量では，（量子）オラクルに対して，質問を重ね合わせてオラクルに問い合わせることが許される．量子オラクル計算モデルにおける効率的な（質問回数が少ない)アルゴリズムが得られれば,効率的な(通信量の少ない）量子分散計算を行うプロトコルが知られている．以下では量子質問計算量に限定する．

F(M)を以下のように定義する．

N 変数論理関数のうち，その論理関数を真にする変数割り当ての数がちょうどＭであるような関数の集合．

例えば，F(0)は恒偽関数のみからなる集合であり，集合F(1)は，2^N個の関数からなる集合である．F(M)は,Ｍだけをパラメータにして，決まる論理関数の集合であり，これらの論理関数同士の類似性は薄いように感じられるが，以下の成果は，論理関数を評価するための質問計算量の範囲が，M の値だけで限定できることを示している．以下では，Ｍが2^Nよりも十分小さいことを仮定する．

集合F(M)に含まれるどのような関数も

$$(N \log M / \log N)^{1/2}$$

程度の量子質問回数で計算可能であることを示した．また，この程度の質問計算量が必要である関数が F(M)に中に含まれているという意味で最適である．この質問回数の値は,Ｍが大きくなれば，かなり大きい値(N に近い値)をとるが，F(M)に含まれるほとんどの関数は，ずっと少ない質問回数で評価可能であることを明らかにした．すなわち，F(M)に含まれるほとんどの関数は，

$$\log M + N^{1/2}$$

程度の量子質問回数で評価可能である．F(M)に含まれるほとんど関数は，$\log M + N^{1/2}$程度の量子質問回数が必要であるという意味において最適である．一方，F(M)に含まれるすべての関数は，

$$N^{1/2}$$

程度の質問計算量が必要であることも示した．

上記の結果から，例えば，具体的な関数の構造を特定するのが難しいケースであっても，「関数を真にする割り当て数」という，シンプルな量がわかりさえすれば，量子質問回数を評価することが可能となる．例えば，グラフのような離散構造のデータがビット列として与えられたとき，その離散構造がある種の性質を満たすかどうかテストするために必要な質問計算量は，一見，難しそうであるが，上記の結果を用いれば，容易に量子質問計算量の存在範囲を限定することが可能になる場合がある．

４．主な発表論文等

〔雑誌論文〕（計７件）

[1] Yasuhiro Takahashi, Seiichiro Tani, Noboru Kunihiro,“Quantum addition circuits and unbounded fan-out.” Proc. the Ninth Asian Conference on Quantum Information Science (AQIS), 査読有, pp.45-46, 2009.

[2] Seiichiro Tani, Masaki Nakanishi, Shigeru Yamashita. “Multi-party quantum communication complexity with routed messages.” IEICE Transactions on Information and Systems, 査読有, E92-D, No.2, pp. 191--199, 2009.

[3] Andris Ambainis, Kazuo Iwama, Masaki Nakanishi, Harumichi Nishimura, Rudy Raymond, Seiichiro Tani, Shigeru Yamashita. “Quantum Query Complexity of Boolean Functions with Small On-Sets.” Proc. 19th International Symposium on Algorithm and Computation (ISAAC’08), 査読有, Lecture Notes in Computer Science, Vol. 5369, pp907-918, Springer, 2008.

[4] Seiichiro Tani, Masaki Nakanishi, Shigeru Yamashita. “Multi-party quantum communication complexity with routed messages.” Proc. 14th Annual Computing and Combinatorics Conference (COCOON’08), 査読有, Lecture Notes in Computer Science, Vol. 5092, pp. 180-190, Springer, 2008.

〔学会発表〕（計１件）

５．研究組織

(1) 研究代表者

谷 誠一郎　(SEIICHIRO TANI)
日本電信電話株式会社ＮＴＴコミュニケーション科学基礎研究所
協創情報研究部　主任研究員
研究者番号：70396183

(2)研究分担者

(3)連携研究者