量子アルゴリズム概観

An Overview of Quantum Algorithms

谷 誠一郎 Seiichiro Tani†

Summary

量子コンピュータは、量子力学の原理を用いて計算を行うコンピュータであり、現在のコンピュータを超える計算能力を発揮することが期待されている。そのためには、量子コンピュータのハードウェアを効果的に使って計算を行うアルゴリズム（量子アルゴリズム）が必要となる。本稿では、これまで行われてきた量子アルゴリズム研究を概観し、課題と展望について議論する。

Key Words

量子コンピュータ, 量子計算, 量子通信, 量子アルゴリズム

1 まえがき

近年、量子コンピュータの実機開発に関する報道が行われるようになってきたが、量子コンピュータの概念が生まれ、そのための研究が始まったのは、30年以上も前のことである。

米国の物理学者 Feynman が、量子力学の法則を利用したコンピュータを作れば、量子シミュレーションを効率的に実行できるのではないかと考えたのが、量子コンピュータの概念の始まりと言われて⁽¹⁾いる。1980年代初期のことである。

一方で、1985年、英国の物理学者 Deutsch が、量子コンピュータの数学モデルとして、万能量子 Turing マシン（万能量子 TM）を定義し⁽²⁾、1989年には、万能量子 TM と理論上等価なモデルである、量子回路モデルを提案した⁽³⁾。更に、1990年代初めには、一般的な立場から量子コンピュータの計算能力を調べる研究も始まった⁽⁴⁾。また、同時期には、Deutsch と Jozsa による量子アルゴリズム⁽⁵⁾、Shor による素因数分解問題／離散対数問題を解く量子アルゴリズム⁽⁶⁾、Grover による量子探索アルゴリズム⁽⁷⁾などが発見され、量子アルゴリズムの研究が注目されるようになった。

量子回路による量子コンピュータの実装は、（量子）ゲート方式と呼ばれている。本稿では、ゲート方式の量子コンピュータ上でのアルゴリズム（以後、量子アルゴリズムと呼ぶ）を扱う。しかしなが

ら、これまで行われてきた量子アルゴリズムの研究は膨大であり（例えば、Quantum Algorithm Zoo⁽⁸⁾には400以上の論文リストがある）、これらを全て網羅することは不可能である。このため、優れた解説論文やサーベイ論文への橋渡しをしつつ、量子アルゴリズム研究の大きな流れを紹介したい。

なお、本稿では、量子力学の原理を用いない、通常のコンピュータ／通信を、古典コンピュータ／古典通信と呼ぶことにする。

2 量子計算モデル

本章では量子計算の数学モデルについて、ごく簡単に解説する。詳細な情報については、標準的な教科書（例えば文献（9））を参照されたい。

n 量子ビットの状態は、数学的には、 2^n 次元複素ベクトル空間 $\mathbb{C}^{2^n}$ の単位ベクトルである。（ $\mathbb{C}$ は複素数の集合を表す。）* 例えば、1 量子ビットの場合、 $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ と表すことにすると、 $\{|0\rangle, |1\rangle\}$ は正規直交基底なので、任意の単位（縦）ベクトルは、 $\alpha|0\rangle + \beta|1\rangle$ と表すことができる（ただし、 $\alpha, \beta \in \mathbb{C}$ かつ $|\alpha|^2 + |\beta|^2 = 1$ ）。特に、 $\{|0\rangle, |1\rangle\}$ を計算基底と呼ぶ。一般に、 n 量子ビットの場合は、次のように定義される基底を計算基底と呼ぶ。まず、 n ビットからなる列 $w = w_{n-1} \cdots w_0$ （ただし、各 $i=0, \dots, n-1$ に対して $w_i \in \{0, 1\}$ ）に対して、 w を 2 進数と見た場合の値を $\text{value}(w) (= \sum_{m=0}^{n-1} 2^m w_m)$ と表記する。次に、 $\text{value}(w) + 1$ 番目の要素だけが 1 で他の要素は 0 である 2^n 次元のベクトルを $|w\rangle$ で表す。このとき、ベクトルの集合 $\{|w\rangle : w \in \{0, 1\}^n\}$ を計算

* 一般的な枠組みでは、 $\mathbb{C}^{2^n}$ 上の半正定値行列でトレースが 1 に規格化されたもの（密度行列と呼ぶ）で表現する。

† NTT コミュニケーション科学基礎研究所、厚木市
NTT Communication Science Laboratories,
NIPPON TELEGRAPH AND TELEPHONE
CORPORATION, Atsugi-shi, 243-0198 Japan

図1 量子ゲートと量子回路

基底と呼ぶ。したがって, n 量子ビットの状態は, $\sum_{w \in \{0,1\}^n} \alpha_w |w\rangle$ と表すことができる (ただし, $\alpha_w \in \mathbb{C}$ かつ $\sum_{w \in \{0,1\}^n} |\alpha_w|^2 = 1$)。基底の取り方は任意であるが, 本稿では計算基底を使うことにする。

n 量子ビットに作用する量子操作は, 大きく分けて二種類ある (図1)。一つは, $\mathbb{C}^{2^n}$ 上のユニタリ変換である。残る一つは, 観測と呼ばれる操作である。対象となるベクトル空間を V とすると, 観測とは, V の部分空間の集合 $\{P_1, \dots, P_m\}$ であって, その直和が V となる ($V = P_1 \oplus \dots \oplus P_m$) ような集合によって特徴付けられる^{*}。量子状態に対して観測を行うことにより, 量子状態は部分空間に射影され, 観測値 (古典情報) が得られる。観測した際に得られる観測値は, どの部分空間に射影されたかによって決まり, 射影先の部分空間 (像空間) は, 量子力学の公理により, 確率的に決まる。例えば, n 量子ビットの状態 $\sum_{w \in \{0,1\}^n} \alpha_w |w\rangle$ に対し, 各計算基底ベクトル $|w\rangle$ で張られる 2^n 個の部分空間で定義される観測を行うと, $|w\rangle$ で張られる部分空間に確率 $|\alpha_w|^2$ で射影され, 観測値 w が得られる。

量子計算の基本的な流れは, まず, 特定の状態 (通常は $|0\rangle$) に初期化した n 個の量子ビットを準備し, $\mathbb{C}^{2^n}$ 上のユニタリ変換 U をかけ, 最後に, あらかじめ決めておいた出力量子ビット (最初に準備した n 量子ビットの一部または全部) を観測する。

ゲート方式の量子コンピュータでは, U を基本ゲートの積に分解しておき, 基本ゲートを量子ビットに作用させていく。ここで基本ゲートとは, 定数個の量子ビットにしか作用しないユニタリ変換のことである。図1に基本ゲートの例を示す。このような量子計算の実現方法は, あたかも論理回路が基本ゲート (AND, OR, NOT など) で構成されているのと類似していることから, 量子回路と呼ばれる。

^{*} 一般的な枠組みでは, $\mathbb{C}^{2^n}$ 上の半正定値行列で表現される線形変換の集合であって, かつ, 和が恒等変換に等しいもの (POVM と呼ぶ) で表す。

上述のとおり, n 量子ビットの状態は, 2^n 個の基底状態 $|w\rangle$ の重ね合わせ $\sum_{w \in \{0,1\}^n} \alpha_w |w\rangle$ として表現される。このため, n 量子ビットを使えば, 2^n 通りの w に対する計算を並列に行えるように見える。しかし, 最後に行う観測により取り出せる古典情報 (観測値) は, 2^n 通りのうちの一つだけであるため, 単純な並列化により高速化できるわけではない。高速計算を実現する量子アルゴリズムとは, 次の条件 [★] を満たす最終状態を生成するユニタリ変換を, 少ない基本ゲートで実現することにほかならない。

[★] 観測したときに, 高確率 (例えば $2/3$ 以上) で, 正しい計算結果に相当する古典情報が得られる。

3 量子コンピュータ単体のアルゴリズム

量子アルゴリズムの時間計算量は, そのアルゴリズムを実装する量子回路に含まれる基本ゲート数 (若しくは量子回路の段数) である。しかし, 時間計算量の解析は一般に容易ではなく, 特に, 「量子アルゴリズムを使えば, どこまで高速化できるか?」という問いに現在の技術で答えるのは極めて困難である。そこで, オラクル計算モデルという, 単純化したモデルが用いられることが多い。

例えば, 関数 $f: X^n \rightarrow Y$ が入力として与えられたとき, f によって決まる値を計算する問題を考える。オラクル計算モデルでは, f が入ったブラックボックス O_f (オラクルと呼ぶ) が与えられ, アルゴリズムが O_f に対して $x \in X^n$ をクエリ (質問) すると, O_f は $f(x)$ をアルゴリズムに返す。これを繰り返すことにより, 必要な入力の情報を得ながら, 計算を進める。また, 量子の場合は, O_f がユニタリ変換であると仮定し, 複数のクエリの重ね合わせ (線形結合) を許す (図2)。

オラクル計算モデルでは, 通常, オラクルへのクエリ (質問) 回数のみを計算量の指標 (質問計算

図2 オラクル計算モデル: f が論理関数の場合の例 (一般の関数の場合も同様に定義可能)

量) とする。質問計算量は、時間計算量の下界を示しているにすぎないが、質問計算量において優れたアルゴリズムが、しばしば、時間計算量の少ない量子アルゴリズムを構築するためのエッセンスを提供する。(例えば、Shor のアルゴリズムの中で、キーとなる量子計算の部分はオラクル計算モデルのアルゴリズムになっている。) また、非自明な下界を解析的に導出することが可能である場合も少なくないため、オラクル計算モデルに基づく量子アルゴリズムの研究は、広く行われてきた。

3.1 代数的アルゴリズム

1990 年代に入ると、ある種の人工的な問題に対して、古典アルゴリズムよりも少ない質問計算量で計算する量子アルゴリズムが発見された^{(4), (5), (10)}。その後間もなく、Shor⁽⁶⁾ は、素因数分解という数学的に自然な問題に対して、既知の古典アルゴリズムよりも指数倍高速な量子アルゴリズムを考案した。大きな数を素因数分解する難しさは、インターネット等で実際に使用されている RSA 暗号の安全性の基礎となっているため、量子コンピュータの登場は、インターネット社会を危険にさらすことを意味する。このため、Shor の結果は、非専門家に対してもインパクトが大きく、多くの人々から量子コンピュータが注目される契機となった。

Shor の素因数分解アルゴリズムの核となる部分は、隠れ部分群問題 (Hidden Subgroup Problem) の特別な場合と理解することができる。

【定義 1】(隠れ部分群問題 (HSP)) H を群 G の未知の部分群とする。また、関数 $f: G \rightarrow Y$ は、 H を法とする各剰余類上では一定値であり、かつ、異なる剰余類に対して異なる値を取るものとする。関数 f がオラクルとして与えられるとき、 H の生成元を求める問題を隠れ部分群問題と呼ぶ。

Kitaev⁽¹¹⁾ は、群 G が可換群のとき、HSP を解く

多項式時間の量子アルゴリズムが存在することを示した。一方、群 G が非可換群の場合、重要な問題が HSP に帰着できることが知られている。例えば、実用的にも理論的にも重要な問題である、グラフ同型性判定問題は、対称群 G に対する HSP に帰着できる。また、耐量子計算機暗号の候補として注目されている格子暗号の理論的根拠となる (ある種の) 最短ベクトル問題は、二面体群 G に対する HSP に帰着できる⁽¹²⁾ (サーベイ論文 (13))。したがって、任意の非可換群 (つまりは対称群) に対する HSP が、量子コンピュータを用いて多項式時間で解ければ、グラフ同型性判定問題が解け、格子暗号が解読できることになる。このため、様々な非可換群の HSP に対する量子アルゴリズムの研究が行われている。文献 (14) は、この種のアルゴリズムについて網羅的に解説しているので参照されたい。しかしながら、一般の非可換群に対する HSP を多項式時間で解く量子アルゴリズムは見つかっていない。

3.2 探索型アルゴリズム

3.2.1 Grover のアルゴリズム

Grover の量子探索アルゴリズム⁽⁷⁾ は、 N 個の候補の中から正解を見つける問題 (探索問題) を高速に解くアルゴリズムである。ここでは、一般性を失うことなく、 N が 2 のべき乗の場合のみを考える。

【定義 2】(探索問題) 関数 $f: \{0,1\}^n \rightarrow \{0,1\}$ がオラクルとして与えられているとき、 $f(x)=1$ を満たす x を求める。ただし、 $N=2^n$ とする。

この問題を解くためには、いかなる古典アルゴリズムもオラクル O_f に $\Omega(N)$ 回クエリすることが必要であるが、Grover の量子アルゴリズムは $O(\sqrt{N})$ 回のクエリで、高確率で答えを見つけることができる。Grover のアルゴリズムは、古典アルゴリズムに対して、二乗のスピードアップしか果たしていないので、Shor のアルゴリズムほどのインパクトは

図3 Element Distinctness 問題と Claw 発見問題 ($\mathbb{Z}_M$ は M を法とする加法群を表す)

ない。しかし、扱う問題の単純さから、因数分解問題（あるいは隠れ部分群問題）に比べ、非常に多くの応用先が考えられる。また、理論的にも、Shor のアルゴリズムは、「既知の」古典アルゴリズムに比べて指数倍高速なのであって、より高速な古典アルゴリズムが将来見つかる可能性は排除されていない。一方、探索問題の古典アルゴリズムの質問計算量 ($\Omega(N)$) は数学的に証明可能である。

Grover の量子アルゴリズムは、様々な形で一般化され、改良が施されてきた^{(15)~(20)}。例えば、位相推定アルゴリズム⁽⁹⁾と組み合わせることで、解の個数 ($f(x)=1$ を満たす x の数) を近似的に計算するアルゴリズム⁽¹⁶⁾や、 f の値が 0/1 ではなく一般の整数値のときに、最小（最大）値を計算するアルゴリズム^{(15), (19)}などがある。また、Grover のアルゴリズムは、量子振幅増幅⁽¹⁶⁾と呼ばれる非常に一般的な枠組みとして定式化できることが示されている。この枠組みを使えば、成功率の低いアルゴリズムから、成功率の高いアルゴリズムを、非常に効率的に作ることができる。例えば、探索問題において、解の数が一つしかない場合を考えると、一度のランダムサンプリングで正解を得る確率は $1/N$ である。この確率を古典的に増幅して、高確率（例えば 99/100）にするには、 $O(N)$ 回の繰返しが必要であるが、量子振幅増幅を使えば、 $O(\sqrt{N})$ 回の繰返しで十分である。（これが Grover のアルゴリズムそのものである。）最近の成果として、アルゴリズムの基本テクニックである動的計画法に対して、Grover のアルゴリズムを用いて更に高速化する新手法が考案された⁽²¹⁾。これにより、巡回セールスマン問題や集合被覆問題などの（指数時間）動的計画アルゴリズムを（指数時間の範囲内ではあるが）高速化できることが示された。

Grover のアルゴリズムは、応用範囲が広いが万能ではない。例えば、ランダムハッシュ関数に基づく暗号への攻撃法に関する問題として、Element Distinctness (ED 問題) を考える（図 3）。ED 問

題の定義において、 $|X|=N$ とするとペア (x, y) の数は $\binom{N}{2} = N(N-1)/2$ なので、Grover のアルゴリズムを適用すると、 $O(\sqrt{N(N-1)/2}) = O(N)$ 回のオラクル・クエリが必要となり、 N 通りの $x \in X$ 全てについてクエリすることとほとんど変わらない。

3.2.2 量子ウォークアルゴリズム

Grover のアルゴリズムではスピードアップが難しい問題に対して、量子ウォーク（ランダムウォークの量子版）を探索に利用するアイデアが生まれた^{(22)~(26)}。例えば、Ambainis⁽²⁶⁾は、ある種のグラフ上における量子ウォークを用いることにより、 $O(N^{2/3})$ 回のオラクル・クエリで ED 問題が解けることを示した。量子ウォークアルゴリズムは、その後、多くの研究^{(27)~(34)}により一般化・改良が進められ、また様々な問題に適用されている。例えば、行列乗算の検証⁽³⁵⁾、三角形発見問題^{(29), (36)~(38)}、バックトラック法の高速化⁽³⁹⁾、claw 発見問題⁽⁴⁰⁾（定義は図 3）などがある。特に、ED 問題と claw 発見問題の量子アルゴリズムは、米国 NIST* が標準化を進めている耐量子計算機暗号の有効な攻撃手法とされており、Ambainis⁽²⁶⁾や Tani⁽⁴⁰⁾のアルゴリズムは、この観点から詳しく分析されている^{(41), (42)}。

量子ウォークを用いたアルゴリズムの具体的な内容については解説論文^{(43), (44)}を参照されたい。量子ウォークは、ランダムウォークの量子版と位置付けられるが、その解析や振舞いは大きく異なる（例えば解説論文⁽⁴⁵⁾）。

3.2.3 半正定値計画法

本節で扱う量子アルゴリズムは、量子質問計算量の下界を与える手法から派生して生まれたものである。Ambainis⁽⁴⁶⁾によって与えられた下界導出法（adversary 法）を一般化し、より強力な下界を与

* National Institute of Standards and Technology. <http://www.nist.gov/>

図4 HHL アルゴリズムが解く問題と計算量

える手法（一般化 adversary 法）が Høyer ら⁽⁴⁷⁾によって考案された。その後、この手法が与える下界は、最適な量子質問計算量と一致する（定数係数を除く、以後も同様）ことが示された^{(48)~(51)}。一般化 adversary 法によれば、解くべき問題 ϕ に対して定義される半正定値計画問題 $P(\phi)$ に対して、その目的関数の最適値が量子質問計算量と一致する。半正定値計画問題は、そのサイズに関する多項式時間で近似的に解けることが知られているが、 $P(\phi)$ のサイズは、 ϕ の入力サイズに対して指数的に大きいため、 $P(\phi)$ を解くことは一般に困難である。また、 $P(\phi)$ が解けたとしても、そこから量子アルゴリズムを得る方法は自明ではない。Reichardt^{(48), (51)} は、線形代数に基づくある種の計算モデル（span program）において、 ϕ を最もコンパクトに表現したときの計算複雑さと $P(\phi)$ の最適値が一致することを発見し、更に、span program から量子ウォークアルゴリズムを得る手法を考案した。これにより、 ϕ を表現する span program $S(\phi)$ を構築できれば、 ϕ を計算する量子アルゴリズムが得られることが明らかになった。（ $S(\phi)$ は ϕ に対して一意ではなく、計算複雑さが低い $S(\phi)$ を見つけることが、効率的な量子アルゴリズムを見つけていることに対応する。）この手法を幾つかの問題に適用することにより、既存の量子アルゴリズムよりも、性能が良い量子アルゴリズムが得られた（例えば (49), (52)~(55)）。ただし、問題 ϕ に応じて、 $S(\phi)$ をアドホックに見つけなければならないため、機械的に量子アルゴリズムが得られるわけではない。

3.2.4 時間計算量に関する議論

Grover のアルゴリズムや量子ウォークアルゴリズムなど、オラクル計算モデルに基づく量子アルゴリズムの性能評価は、前述のとおり、オラクルに対

するクエリ数（質問計算量）で行う。しかし、アルゴリズム全体の時間計算量としては、クエリ以外の計算に要するステップ数を加える必要がある。

Grover のアルゴリズムを単純適用するようなケースでは、全体の時間計算量は、クエリの回数と大きく変わらない ($\sqrt{N} (\log N)^{O(1)}$ のオーダー) が、種々の問題に応じて変更を加えながら使う場合はこの限りではない。また、アルゴリズム部分を物理的に実装することを考えた場合、量子ビットは、物理的制約から一次元や二次元、若しくは三次元に配置されることが想定される。この場合、隣接量子ビット間でしか、2 量子ビット操作を行えない物理系では、より多くの時間が掛かってしまう可能性があるので注意が必要である。

オラクル部分を実装する手法についても研究が進んでいるが⁽⁵⁶⁾、オラクル計算モデルは、別の量子アルゴリズムの計算結果をメインの量子アルゴリズムで使う構成をモデル化したものとも考えることができる。この場合、オラクル O_f に対して x をクエリすると、実際には、別の量子アルゴリズム $\mathcal{A}_x$ が動作し、その結果を $f(x)$ の値として返す。これにより、再帰を用いた量子アルゴリズムのモデル化も可能となる。

3.3 線形方程式のアルゴリズム

Harrow, Hassidim, Lloyd (HHL)⁽⁵⁷⁾ は、量子シミュレーションと位相推定アルゴリズム⁽⁹⁾を応用することで、線形方程式 $Ax=b$ の解 x を出力する量子アルゴリズムを考案した（図4）。ここで、 A は $N \times N$ 対称行列、 b は N 次元実ベクトルである。 A の非零要素が少なく（疎行列）かつ、 A の条件数 κ が小さい場合、HHL アルゴリズムは、 $\log N$ の多項式

* A の [絶対値における] 最小固有値に対する最大固有値の比

図5 ハイブリッド最適化（量子ヒューリスティック）

に比例する時間で計算を終える。（条件数や誤り率に対する依存性に関して改良が進められている。⁽⁵⁸⁾⁽⁵⁹⁾）ただし、HHL アルゴリズムが出力する $\mathbf{x}$ や定数ベクトル $\mathbf{b}$ は、 $O(\log N)$ 量子ビットの量子状態としての $|\mathbf{x}\rangle$ 及び $|\mathbf{b}\rangle$ である点に注意する必要がある。 $|\mathbf{x}\rangle = \alpha \sum_{i=1}^N x_i |i\rangle$ (α は正規化係数) を観測しても、ある x_i のみが分かるだけなので、例えば、 $\mathbf{x} = (x_1, \dots, x_N)^T$ を得るためには、 $\Omega(N)$ 回繰り返す必要がある。しかし、 $\mathbf{x}$ の統計的な情報のみが必要な場合は、HHL アルゴリズムは非常に有効である可能性がある。線形方程式は数多くの応用があるので、HHL アルゴリズムに対する期待は大きい。ただし、HHL アルゴリズムが高速に動作するためには、ほかに幾つか条件があり、注意が必要である⁽⁶⁰⁾。例えば、定数部分 $|\mathbf{b}\rangle$ を短時間で準備できるかどうかは自明ではない。

線形方程式を更に一般化した、半正定値計画法に対する量子アルゴリズム⁽⁶¹⁾⁽⁶²⁾ も研究が進んでおり、注目すべき研究テーマの一つになっている。

3.4 量子ヒューリスティック

これまで、量子アルゴリズムの研究は、量子回路などの理論モデル上で解析的に研究が行われてきた。つまり、サイズ N に対して、 $O(\sqrt{N})$ 時間で問題を解くなどと言うように、理論的に必要な計算量が保証されるものを量子アルゴリズムと呼んできた。しかし、近年、量子コンピュータの実機開発が行われるようになり、理論的な性能保証がない「量子ヒューリスティック」の提案も行われるようになってきている。多くは、図5のように古典コンピュータと量子コンピュータのハイブリッド型で最適化問題を解く形式である。このため、比較的小規模の量子コンピュータでも効果が上がることが期待されているが、実証はこれからである。例えば、

QVE (Quantum Variational Eigensolver)⁽⁶³⁾ は、エルミート行列の最小固有ベクトルを近似的に計算するために、Rayleigh-Ritz 商を最小化するベクトルを逐次改善手法で探索する。このとき、Rayleigh-Ritz 商を計算する部分だけを量子コンピュータに実行させ、解を改善する部分は古典コンピュータが行う。応用としては、量子化学計算分野などへの適用が期待されている。また、最適化の一般的な枠組みとして QAOA (Quantum Approximate Optimizing Algorithm)⁽⁶⁴⁾ や、学習によって量子回路を最適化する量子回路学習⁽⁶⁵⁾ という手法などが提案されている。更に、機械学習アルゴリズムを量子コンピュータにより加速する研究も注目されている（詳細は文献⁽⁶⁶⁾）。

4 量子通信を伴うアルゴリズム

分散計算とは、ネットワーク上の複数のコンピュータが、ローカルな計算と通信を繰り返して行う計算である。通常、ローカルな計算コストよりも通信コスト（通信ビット数、通信回数等）の影響の方が大きいので、通信コストを抑えることが主な興味の対象となる。

4.1 2 台のコンピュータによる関数計算

コンピュータ A と B がそれぞれローカルに持っているデータ x と y (ともに n ビットとする) が等しいか確認したい。もちろん、一方が他方にデータを全部送ってしまえば簡単であるが、 x と y が巨大なファイルである場合は、多大な通信コストが掛かるので好ましくない。量子通信を用いたとしても、単純に送信する手段に訴える限りは、状況はほとんど改善しないことが次の定理から分かる。

図6 複数台のコンピュータによる関数計算

【定理 3】 (文献 (67), (68)) A から B へ n ビットのメッセージを双方向通信路で送るためには、少なくとも $n/2$ 量子ビットを A から B へ送信する必要がある、かつ、 AB 間のトータルの量子通信量は、少なくとも n 量子ビットである。

実は、小さな誤り確率 (例えば $1/n^{100}$) を許せば、 $O(\log n)$ ビットの通信で x と y が等しいかどうかを確認できる古典アルゴリズムが知られている⁽⁶⁹⁾。このように複数のコンピュータ $A, B, C, \dots$ が、それぞれローカルに持っている入力データ $x, y, z, \dots$ に対する関数 f の値を計算したいとき、(関数 f に依存して) アルゴリズムを工夫することにより、単純に全データを送るよりも、通信コストを大幅に抑えられる場合がある。量子通信を用いると、全データを送るよりも、より一層、通信量を削減できる場合があることも知られている⁽⁷⁰⁾。

ネットワークに参加するコンピュータの数を 2 や 3 に限定したり、完全結合のネットワークだけを考えたりすることにより、ネットワークの形状よりも、関数 f に対する通信コストの依存性に焦点を絞って研究する分野は、通信計算量 (communication complexity) と呼ばれ、古典・量子の双方において、精力的に研究されている。このような問題設定にするのは、通信計算量の分野は、回路計算量や質問計算量などのほかの理論計算機科学分野の問題に対する答えを得ることを主な動機としているからである。詳細については、通信計算量の教科書⁽⁶⁹⁾ や解説論文^{(70), (71)} (量子の通信計算量も含む) を参照されたい。

4.2 多数のコンピュータによる関数計算

計算に参加するコンピュータ数が多くなってくると、それらを接続するネットワークの形状も様々なものが考えられる。その形状に関する情報が与えられていれば、それを利用して効率的なアルゴリズム

ムを作ることができる。また、ネットワークの形状が分からなくても、コンピュータ数の上限 N が分かっているならば、ネットワークの直径 (最も離れた 2 台のコンピュータ間のホップ数) は高々 N であることを利用することができる。このように、多数のコンピュータが参加する場合においては、ネットワークの性質と計算すべき関数の双方を考慮して、アルゴリズムを構成することが重要となる。

計算と通信を量子にすることにより、古典の場合の限界を超えて、通信コストを低減できる場合があることが知られている。例えば、図 6 のように、 n 台のコンピュータ $P_1, \dots, P_n$ がリング状のネットワークで接続されているとする。各コンピュータ P_i には、それぞれ、 $l=O(\log n)$ ビットのデータ x_i が入力として与えられている。これら n 個の l ビット列に重複がないことをチェックする問題を考える。計算と通信が古典の場合、この問題を高確率で解くためには $\Omega(n^2)$ ビットの通信が必要であるが、計算と通信がともに量子の場合は、 $O(n\sqrt{n})$ 量子ビットで解くアルゴリズムが知られている⁽⁷²⁾。このアルゴリズムのアイデアは、「条件 (★): ある $j \in \{1, \dots, n\}$ に対して $x_i = x_j$ である」を満たす $i \in \{1, \dots, n\}$ が存在するか否かを Grover の探索アルゴリズムを用いて確認するというシンプルなものである。ただし、条件 (★) が満たされれば 1 を返し、満たされなければ 0 を返す関数 $f: \{1, \dots, n\} \rightarrow \{0, 1\}$ に対するオラクルは与えられていないので、同じ役目を果たすサブルーチンを、通信やローカルな計算を用いて構築する必要がある。このように Grover のアルゴリズムを分散環境で用いる手法は、ネットワークの直径を計算する問題⁽⁷³⁾ などにも使われ、古典の場合の限界を超えて、通信ラウンド数削減が可能であることが示された。

4.3 状態遷移を目的とする分散計算

一般の分散計算は、必ずしも関数を計算するものばかりではない。例えば、リーダー選挙問題、デッドロック検出問題、全域木構築問題、ビザンチン合意問題などがある^{(74), (75)}。いずれも、実際のネットワークを運用する上での課題を動機としたものである。研究の取組み方は、理論的なものから実践的なものまで幅広い。ここでは、特に基本的と思われる、リーダー選挙問題を取り上げ、その量子アルゴリズムについて解説する。

4.3.1 リーダー選挙問題

この問題の目的は、複数のコンピュータが「リー

図7 リーダー選挙問題

ダー」となる一台を決めること、すなわち、リーダー役が不在である「初期状態」から、リーダーがちょうど一台だけいる「最終状態」にシステム全体を移行させることである(図7)。各コンピュータがMAC(Media Access Control)アドレスのような一意性のあるアドレスを持っているという仮定の下では、最大のMACアドレス値を持つコンピュータを特定する問題に帰着することができる。(この問題については、多くの研究があるが、本稿では詳細に立ち入らない。)

一方、一意性のあるアドレスを常に保証することは、実用上、厳しい制約となる場合があることから、このようなアドレスを持たないコンピュータ同士の分散計算も重要な研究テーマになっている。Angluin⁽⁷⁶⁾は、一切区別できない古典コンピュータ同士で構成されるネットワーク上での分散計算を創始した。このようなネットワークを「匿名古典ネットワーク(anonymous network)」と呼ぶ*。Angluinは、無限に多くの匿名古典ネットワークに対して、リーダー選挙問題を解く決定性アルゴリズムが存在しないことを示した。更に、Yamashita-Kameda⁽⁷⁷⁾は、「匿名古典ネットワーク上のコンピュータ数が与えられた場合に、決定性アルゴリズムによりリーダーを決定できる」ための必要十分条件を与えた。例えば、リング、完全グラフ、ある種の正則グラフに対応する匿名古典ネットワークでは、リーダー選挙は不可能であることが導かれる。匿名古典ネットワークにおいて決定的にはリーダーを選べない直感的な理由は以下のとおりである(厳密には、注意深い議論が必要である)：

全てのコンピュータは、全く同じプログラムを実行しているはずである。なぜなら、異なるプログラ

ムを実行する2台が存在したとすれば、それらのプログラムのコードを識別子とみなすことにより、区別可能になり、仮定に反するからである。同じプログラムを実行するコンピュータは同じ最終状態になるはずで、これではリーダーは決定できない。

なお、匿名古典ネットワークにおけるリーダー選挙に関する他の研究成果に関しては文献(78)、(79)の参考文献を参照されたい。また、亀田・山下による教科書⁽⁷⁴⁾にも分かりやすい解説がある。

4.3.2 リーダー選挙を行う量子アルゴリズム

匿名古典ネットワークで行われる計算と通信を量子計算と量子通信に置き換えることで、匿名「量子」ネットワークを定義する。そして、「匿名量子ネットワークにおける分散量子計算では、リーダー選挙問題を決定的に解くことができる」というのが本節の主題である。ここで、「量子計算で決定的に解く」とは、決められた時間内に確率1でリーダーを決定することである。定理の形で書くと以下のようになる。

[定理4] (文献(80)、(81)) 任意形状の匿名量子ネットワーク上において、コンピュータ数 n の上界 N が各コンピュータに与えられたとき、リーダーを確率1で決定する量子アルゴリズムが存在する。このとき、各コンピュータは、ネットワークの形状を知る必要がない。また、上記アルゴリズムが通信する量子ビット数は $O(n^2N^2)$ でバウンドされる。特に、同期型ネットワークでは $O(N^2)$ ラウンドで上記アルゴリズムは終了する。

前述のとおり、匿名古典ネットワークでは、コンピュータ数 n が正確に与えられていても決定的にはリーダー選挙できないネットワークが無限に多く存在する。定理4が示す内容は、これとは全く対称的であり、また、(暗号プロトコルを除く)ほかの様々な量子アルゴリズムが、計算時間・通信量な

* 通常、単に、匿名ネットワークと呼ばれるが、本稿では、量子版との区別を明確にするため、匿名古典ネットワークと呼ぶ。また、ここでいう「匿名」は、暗号・セキュリティ分野における「匿名性」とは全く関係がない。

どの計算コストの「量」という点で古典アルゴリズムよりも優位であることを主張していることと比較しても、特徴的である。実際、定理4の量子アルゴリズムは、自然な問題において、量子計算の「質」的な優位性を示した世界初の例になっている。

ただし、定理4は、極めて理想的な量子コンピュータ・量子ネットワークに対して得られる理論的な結果であることを断っておきたい。実際には、量子演算デバイスの精度限界があり、また、雑音の影響も受けることから、確率1で解けることはあり得ない。しかし、このことは、古典の世界において確率1では解けない状況と本質的に異なる。なぜなら、実際の量子コンピュータ・量子ネットワークを用いた場合に、成功確率がどれだけ1から離れるかは、実装に起因する誤りだけに依存するが、古典の場合は、原理的な理由によって成功確率が1とはならないためである。

5 あとがき

残念ながら、本稿で紹介できなかった話題はたくさんある。例えば、量子シミュレーションを行うためのアルゴリズムや非万能量子計算モデル上でのアルゴリズムの研究については、文献(82)によるサーベイ及びその参考文献を参照されたい。また、PAC学習などに代表される計算理論的学习に関する量子アルゴリズムの研究については解説論文⁽⁸³⁾を、膨大なデータの性質を高速に検査する手法(quantum property testing)についてはサーベイ論文⁽⁸⁴⁾を参照されたい。

■ 文献

- (1) R.P. Feynman, "Simulating physics with computers," Int. J. Theor. Phys., vol.21, no.6-7, pp.467-488, June 1982.
- (2) D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," Proc. R. Soc. A, vol.400, no.1818, pp.97-117, July 1985.
- (3) D. Deutsch, "Quantum computational networks," Proc. R. Soc. A, vol.425, no.1868, pp.73-90, Sept.1989.
- (4) E. Bernstein and U.V. Vazirani, "Quantum complexity theory," SIAM J. Comput., vol.26, no.5, pp.1411-1473, Oct.1997.
- (5) D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," Proc. R. Soc. Lond. A, vol.439, pp.553-558, July 1992.
- (6) P.W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol.26, no.5, pp.1484-1509, Oct.1997.

- (7) L.K. Grover, "A fast quantum mechanical algorithm for database search," Proc. 28th Annual ACM Symp. Theory of Computing (STOC), pp.212-219, July 1996.
- (8) "Quantum algorithm zoo," <https://quantumalgorithmzoo.org/>
- (9) M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
- (10) D.R. Simon, "On the power of quantum computation," SIAM J. Comput., vol.26, no.5, pp.1474-1483, Oct.1997.
- (11) A.Y. Kitaev, "Quantum measurements and the abelian stabilizer problem," arXiv e-prints, quant-ph/9511026, Nov.1995.
- (12) O. Regev, "Quantum computation and lattice problems," SIAM J. Comput., vol.33, no.3, pp.738-760, March 2004.
- (13) H. Kobayashi and F. Le Gall, "Dihedral hidden subgroup problem: A survey," Information and Media Technologies, vol.1, no.1, pp.178-185, 2006.
- (14) A.M. Childs and W. van Dam, "Quantum algorithms for algebraic problems," Rev. Mod. Phys., vol.82, pp.1-52, Jan. 2010.
- (15) C. Dürr and P. Høyer, "A quantum algorithm for finding the minimum," arXiv e-prints, quant-ph/9607014, July 1996.
- (16) G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," Quantum Computation and Information, vol.305, pp.53-74, Contemporary Mathematics, American Mathematical Society, 2002.
- (17) P. Høyer, M. Mosca, and R. de Wolf, "Quantum search on bounded-error inputs," Proc. 30th Int. Colloq. on Automata, Languages and Programming (ICALP), pp.291-299, June 2003.
- (18) S. Aaronson and A. Ambainis, "Quantum search of spatial regions," Theory of Computing, vol.1, no.1, pp.47-79, July 2005.
- (19) C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla, "Quantum query complexity of some graph problems," SIAM J. Comput., vol.35, no.6, pp.1310-1328, June 2006.
- (20) A. Ambainis, "Quantum search with variable times," Theory Comput. Syst., vol.47, no.3, pp.786-807, Oct. 2010.
- (21) A. Ambainis, K. Balodis, J. Iraids, M. Kokainis, K. Prūsis, and J. Vihrovs, "Quantum speedups for exponential-time dynamic programming algorithms," Proc. 30th Annual ACM-SIAM Symp. Discrete Algorithms (SODA), pp.1783-1793, Jan.2019.
- (22) N. Shenvi, J. Kempe, and K.B. Whaley, "Quantum random-walk search algorithm," Phys. Rev. A, vol.67, no.5, 052307, May 2003.
- (23) A.M. Childs and J. Goldstone, "Spatial search by quantum walk," Phys. Rev. A, vol.70, no.2, p.022314, Aug.2004.
- (24) M. Szegedy, "Quantum speed-up of markov chain based algorithms," Proc. 45th Annual IEEE Symp. Foundations of Computer Science (FOCS), pp.32-41, Oct. 2004.
- (25) A. Ambainis, J. Kempe, and A. Rivosh, "Coins

- make quantum walks faster,” Proc 16th Annual ACM-SIAM Symp. Discrete Algorithms (SODA), pp.1099–1108, Jan. 2005.
- (26) A. Ambainis, “Quantum walk algorithm for element distinctness,” SIAM J. Comput., vol.37, no.1, pp.210–239, May 2007.
 - (27) F. Magniez, A. Nayak, J. Roland, and M. Santha, “Search via quantum walk,” SIAM J. Comput., vol.40, no.1, pp.142–164, Feb. 2011.
 - (28) F. Magniez, A. Nayak, P.C. Richter, and M. Santha, “On the hitting times of quantum versus random walks,” Algorithmica, vol.63, no.1-2, pp.91–116, June 2012.
 - (29) S. Jeffery, R. Kothari, and F. Magniez, “Nested quantum walks with quantum data structures,” Proc. 24th Annual ACM-SIAM Symp. Discrete Algorithms (SODA), pp.1474–1485, Jan. 2013.
 - (30) A. Belovs, A.M. Childs, S. Jeffery, R. Kothari, and F. Magniez, “Time-efficient quantum walks for 3-distinctness,” Proc. 40th Int. Colloq. Automata, Languages, and Programming (ICALP), Part I, pp.105–122, July 2013.
 - (31) H. Krovi, F. Magniez, M. Ozols, and J. Roland, “Quantum walks can find a marked element on any graph,” Algorithmica, vol.74, no.2, pp.851–907, Feb. 2016.
 - (32) C. Dohotaru and P. Høyer, “Controlled Quantum Amplification,” Proc. 44th Int. Colloq. Automata, Languages, and Programming (ICALP), pp.18:1–18:13, July 2017.
 - (33) A. Ambainis, A. Gilyén, S. Jeffery, and M. Kokainis, “Quadratic speedup for finding marked vertices by quantum walks,” arXiv e-prints, arXiv:1903.07493, March 2019.
 - (34) S. Apers, A. Gilyén, and S. Jeffery, “A unified framework of quantum walk search,” arXiv e-prints, arXiv:1903.07493, 2019.
 - (35) H. Buhrman and R. Špalek, “Quantum verification of matrix products,” Proc. 17th Annual ACM-SIAM Symp. Discrete Algorithms (SODA), pp.880–889, Jan. 2006.
 - (36) F. Magniez, M. Santha, and M. Szegedy, “Quantum algorithms for the triangle problem,” SIAM J. Comput., vol.37, no.2, pp.413–424, May 2007.
 - (37) T. Lee, F. Magniez, and M. Santha, “Improved quantum query algorithms for triangle finding and associativity testing,” Proc. 24th Annual ACM-SIAM Symp. Discrete Algorithms (SODA), pp.1486–1502, Jan. 2013.
 - (38) F. Le Gall, “Improved quantum algorithm for triangle finding via combinatorial arguments,” Proc. 55th IEEE Annual Symp. Foundations of Computer Science (FOCS), pp.216–225, Oct. 2014.
 - (39) A. Montanaro, “Quantum-walk speedup of backtracking algorithms,” Theory of Computing, vol.14, no.15, pp.1–24, Dec. 2018.
 - (40) S. Tani, “Claw finding algorithms using quantum walk,” Theor. Comput. Sci., vol.410, no.50, pp.5285–5297, Nov. 2009.
 - (41) J. Czajkowski, L. Groot Bruinderink, A. Hülsing, C. Schaffner, and D. Unruh, “Post-quantum security of the sponge construction,” Proc. 9th Int. Conf. Post-Quantum Cryptography (PQcrypto), pp.185–204, April 2018.
 - (42) S. Jaques and J.M. Schanck, “Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE,” Proc. 39th Annual Int. Cryptology Conf. (CRYPTO), pp.32–61, Aug. 2019.
 - (43) A. Ambainis, “Quantum walks and their algorithmic applications,” Int. J. Quantum Inf., vol.1, no.04, pp.507–518, Dec. 2003.
 - (44) M. Santha, “Quantum walk based search algorithms,” Proc. 5th Theory and Applications of Models of Computation (TAMC), pp.31–46, April 2008.
 - (45) J. Kempe, “Quantum random walks: an introductory overview,” Contemp. Phys., vol.44, no.4, pp.307–327, 2003.
 - (46) A. Ambainis, “Quantum lower bounds by quantum arguments,” J. Comput. Syst. Sci., vol.64, no.4, pp.750–767, June 2002.
 - (47) P. Høyer, T. Lee, and R. Špalek, “Negative weights make adversaries stronger,” Proc. 39th Annual ACM Symp. Theory of Computing (STOC), pp.526–535, June 2007.
 - (48) B. Reichardt, “Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean function,” Proc. 50th Annual IEEE Symp. Foundations of Computer Science (FOCS), pp.544–551, April 2009.
 - (49) B.W. Reichardt, “Reflections for quantum query algorithms,” Proc. 22nd Annual ACM-SIAM Symp. Discrete Algorithms (SODA), pp.560–569, Jan. 2011.
 - (50) T. Lee, R. Mittal, B.W. Reichardt, R. Špalek, and M. Szegedy, “Quantum query complexity of state conversion,” Proc. IEEE 52nd Annual Symp. Foundations of Computer Science (FOCS), pp.344–353, Oct. 2011.
 - (51) B.W. Reichardt, “Span programs are equivalent to quantum query algorithms,” SIAM J. Comput., vol.43, no.3, pp.1206–1219, May 2014.
 - (52) B.W. Reichardt and R. Špalek, “Span-program-based quantum algorithm for evaluating formulas,” Proc. 40th annual ACM symp. Theory of computing (STOC), pp.103–112, May 2008.
 - (53) A. Belovs and B.W. Reichardt, “Span programs and quantum algorithms for st-connectivity and claw detection,” Proc. 20th Annual European Symp. Algorithms (ESA), pp.193–204, March 2012.
 - (54) A. Belovs, “Span programs for functions with constant-sized 1-certificates: extended abstract,” Proc. 44th Symp. Theory of Computing (STOC), pp.77–84, May 2012.
 - (55) A. Belovs, “Learning-graph-based quantum algorithm for k-distinctness,” Proc. 53rd Annual IEEE Symp. Foundations of Computer Science (FOCS), pp.207–216, Oct. 2012.
 - (56) V. Giovannetti, S. Lloyd, and L. Maccone, “Quantum random access memory,” Phys. Rev. Lett., vol.100, no.16, p.160501, April 2008.
 - (57) A.W. Harrow, A. Hassidim, and S. Lloyd, “Quantum algorithm for linear systems of equations,” Phys. Rev. Lett., vol.15, no.103, 150502, Oct. 2009.
 - (58) A. Ambainis, “Variable time amplitude

- amplification and quantum algorithms for linear algebra problems,” Proc. 29th Int. Symp. Theoretical Aspects of Computer Science (STACS), pp.636–647, Feb. 2012.
- (59) A.M. Childs, R. Kothari, and R.D. Somma, “Quantum algorithm for systems of linear equations with exponentially improved dependence on precision,” SIAM J. Comput., vol.46, no.6, pp.1920–1950, Dec. 2017.
- (60) S. Aaronson, “Read the fine print,” Nat. Phys., vol.11, no.4, pp.291–293, April 2015.
- (61) F.G.S.L. Brandao and K.M. Svore, “Quantum speed-ups for solving semidefinite programs,” Proc 58th Annual IEEE Symp. Foundations of Computer Science (FOCS), pp.415–426, Oct. 2017.
- (62) J. van Apeldoorn and A. Gilyén, “Improvements in Quantum SDP-Solving with Applications,” Proc. 46th Int. Colloq. Automata, Languages, and Programming (ICALP), Part I, pp.99:1–99:15, July 2019.
- (63) A. Peruzzo, J. McClean, P. Shadbolt, M.H. Yung, X.Q. Zhou, P.J. Love, A. Aspuru-Guzik, and J.L. O’Brien, “A variational eigen-value solver on a photonic quantum processor,” Nat. Commun., vol.5, p.4213, July 2014.
- (64) E. Farhi, J. Goldstone, and S. Gutmann, “A Quantum Approximate Optimization Algorithm,” arXiv e-prints, arXiv:1411.4028, 2014.
- (65) K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, “Quantum circuit learning,” Phys. Rev. A, vol.98, no.3, 032309, 2018.
- (66) J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” Nature, vol.549, no.7671, pp.195–202, 2017.
- (67) A.S. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” Problemy Peredachi Informatsii, vol.9, no.3, pp.3–11, 1973. (English Translation in Problems of Information Transmission, 9:177–183, 1973.)
- (68) R.E. Cleve, W. van Dam, M. Nielsen, and A. Tapp, “Quantum entanglement and the communication complexity of the inner product function,” Proc. First NASA Int. Conf. Quantum Computing and Quantum Communications, pp.61–74, 1998.
- (69) E. Kushilevitz and N. Nisan, Communication Complexity, Cambridge University Press, Cambridge, 1997.
- (70) 谷 誠一郎, フランソワ・ルガル, “量子分散コンピューティング,” 信学論 (A), vol.J90-A, no.5, pp.393–402, May 2007.
- (71) R. de Wolf, “Quantum communication and complexity,” Theor. Comput. Sci., vol.287, no.1, pp.337–353, Sept. 2002.
- (72) S. Tani, M. Nakanishi, and S. Yamashita, “Multi-party quantum communication complexity with routed messages,” IEICE Trans. Inf. & Syst., vol. E92-D, no.2, pp.191–199, Feb. 2009.
- (73) F. Le Gall and F. Magniez, “Sublinear-time quantum computation of the diameter in congest networks,” Proc. 37th ACM Symp. Principles of Distributed Computing (PODC), pp.337–346, July 2018.
- (74) 亀田恒彦, 山下雅史, 分散アルゴリズム, 近代科学社, 東京, 1994.
- (75) N.A. Lynch, Distributed Algorithms, Morgan Kaufman Publishers, Burlington, 1996.
- (76) D. Angluin, “Local and global properties in networks of processors (extended abstract),” Proc. 12th Annual ACM Symp. Theory of Computing (STOC), pp.82–93, April 1980.
- (77) M. Yamashita and T. Kameda, “Computing on an anonymous network,” Proc. 7th Annual ACM Symp. Principles of Distributed Computing (PODC), pp.117–130, 1988.
- (78) Y. Afek and Y. Matias, “Elections in anonymous networks,” Inf. Comput., vol.113, no.2, pp.312–330, Sept. 1994.
- (79) M. Yamashita and T. Kameda, “Computing on anonymous networks: Part I – characterizing the solvable cases,” IEEE Trans. Parall. Distrib. Syst., vol.7, no.1, pp.69–89, Jan. 1996.
- (80) S. Tani, H. Kobayashi, and K. Matsumoto, “Exact quantum algorithms for the leader election problem,” Proc. 22nd Symp. Theoretical Aspects of Computer Science (STACS ’05), pp.581–592, Feb. 2005.
- (81) S. Tani, H. Kobayashi, and K. Matsumoto, “Exact quantum algorithms for the leader election problem,” ACM T. Comput. Theor., vol.4, no.1, pp.1–24, March 2012.
- (82) A. Montanaro, “Quantum algorithms: an overview,” npj Quantum Information, vol.2, p.15023, Jan. 2016.
- (83) S. Arunachalam and R. de Wolf, “Guest column: A survey of quantum learning theory,” SIGACT News, vol.48, no.2, pp.41–67, June 2017.
- (84) A. Montanaro and R. de Wolf, “A survey of quantum property testing,” no.7, Graduate Surveys, Theory of Computing Library, July 2016. <http://www.theoryofcomputing.org/library.html>

((2020 年 1 月 30 日受付, 3 月 30 日再受付))

谷 誠一郎 (正員: シニア会員)

1993 京大・工・情報工卒. 1995 東大院・理・情報科学了. 博士 (情報理工学). 1995 日本電信電話株式会社入社. 2004 ~ 09 JST ERATO 今井量子計算機構プロジェクト研究員 (兼任). 2010 ~ 11 Waterloo 大学量子計算研究所客員研究員. 理論計算機科学, 特に, 量子アルゴリズム, 量子計算量理論, 分散計算の研究に従事. 2000 年度本会情報・システムソサイエティ論文賞, 2018 年度本会業績賞各受賞. 情報処理学会, IEEE, ACM 各会員.