

# 基礎から学ぶ量子計算 アルゴリズムと 計算量理論

5.7 通信を含む計算問題に対する量子プロトコル

5.8 そのほかの量子アルゴリズム

松本侑真 中西泰一

2023/11/27

1/7

# 通信を含む計算問題に対するプロトコル

## 背景

- 入力が複数のパーティ（人）に分割されている環境において、何らかのタスクを実行する状況はデータが大規模化した今日ではよく表れる。
- そのような状況下において問題を解くためのモデルの重要性が高まっている。

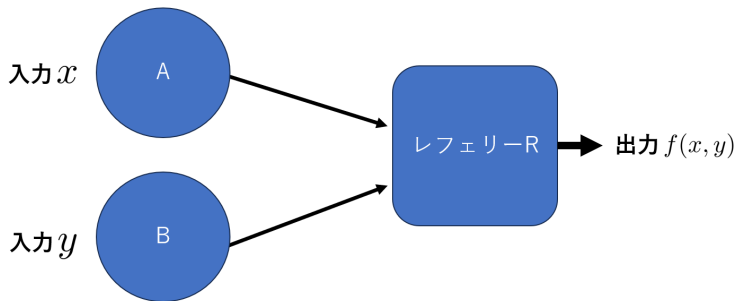
このようなモデルのうち最も簡素なものが**同時メッセージパッシングモデル：SMP モデル**

# 定義5.1（同時メッセージパッシングモデル）

## 設定

- Aは入力  $x \in \{0, 1\}^n$ 、Bは入力  $y \in \{0, 1\}^n$  を持つ。
- レフェリーRは入力を持たないが、AおよびBはRにメッセージを送ることができる。
- AとBは互いにメッセージを送ることができないし、RからAやBにメッセージを送ることもできない。
- さらに、A、B、Rで共有するものは何もない。

## 定義5.1 (同時メッセージパッシングモデル)



### 目的

レフェリー R が  $f(x, y)$  を出力する。ここで、関数  $f$  は A、B、R すべてにとって既知とする。

# 定義5.1（同時メッセージパッシングモデル）

## 計算量

- AおよびBがRに送るメッセージ長の和（ビット数の和）のみ考慮する。
- 関数  $f$  の通信計算量とは、 $f(x, y)$  を計算するA、B、Rのアルゴリズム（通信プロトコル）すべてにおいて計算量が最小となるような通信プロトコルの計算量を指す。

# 等価性関数 (equality function)

SMP モデルにおける代表的な関数  $f$  の 1 つが等価性関数  $EQ_n: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  であり、

$$EQ_n(x, y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases} \quad (1)$$

と定義される。

## 定理 5.10 (Buhrman-Cleve-Watrous-de Wolf)

$EQ_n$  を成功確率  $2/3$  以上で解くための量子通信計算量は  $\mathcal{O}(\log n)$  である。

古典的なメッセージ送信のみで  $EQ_n$  を成功確率  $2/3$  以上で解くための通信計算量は  $\Omega(\sqrt{n})$  であることが知られている。

# その他の量子アルゴリズム

本章で紹介してきた量子アルゴリズムは2000年代の初期までには発見されていた。現在ではより複雑な量子アルゴリズムのサブルーチンとしてや、古典アルゴリズムとの組み合わせとして使われている。

- ランダムウォークの量子版である量子ウォークを用いたアルゴリズム
- 連立一次方程式を高速に解く HHL アルゴリズム
- 行列の特異値分解をもとにした量子特異値変換アルゴリズム

などが比較的応用範囲が広いアルゴリズムである。