Quantum communication complexity of linear regression

Changpeng Shao

Academy of Mathematics and Systems Science, Chinese Academy of Sciences
based on joint work with Ashley Montanaro
arXiv:2210.01601

INFORMS Optimization Society Conference
22-24 March 2024

Background

Quantum computers can solve some problems much faster than classical computers. For example, quantum computers could be good at solving linear algebra problems.

Background

Quantum computers can solve some problems much faster than classical computers. For example, quantum computers could be good at solving linear algebra problems.

A fundamental problem:

> **Solving linear system.**
> **Given some quantum access to a matrix $A \in \mathbb{R}^{m\times n}$, and the ability to prepare $|\mathrm{b}\rangle$, output $|A^{-1}\mathrm{b}\rangle$.**

Here A^{-1} means the pseudoinverse if it is not invertible.

Quantum algorithms for linear systems

Theorem (Harrow, Hassidim, Lloyd 2008 + many others[1])
There is a quantum algorithm that solves this problem in cost

$$\kappa \cdot \mathrm{poly}(\log(mn), \log 1/\varepsilon),$$

where κ is the condition number.

Leads to wide applications, especially in machine learning, e.g., recommendation systems [Kerenidis and Prakash, 1603.08675].

[1] [Ambainis 1010.4458], [Childs, Kothari, Somma 1511.02306], [Wossnig, Zhao, Prakash 1704.06174], [Chakraborty, Gilyén, Jeffery 1804.01973], ...

Quantum-inspired classical algorithms

In 2018, Tang showed that assuming a similar data structure to QRAM, there is a classical algorithm that can solve the recommendation systems in time polylog in the dimension. [Tang, 1807.04271].

Quantum-inspired classical algorithms

In 2018, Tang showed that assuming a similar data structure to QRAM, there is a classical algorithm that can solve the recommendation systems in time polylog in the dimension. [Tang, 1807.04271].

$\Rightarrow$ no quantum exponential speedups for many machine learning problems in the low-rank case. [Chia et al, 1910.06151].

Quantum communication complexity of linear regressions

To explore quantum speedups, we are usually more interested in

- Time complexity
- Query complexity
- Communication complexity
- ...

Quantum communication complexity of linear regressions

To explore quantum speedups, we are usually more interested in

- Time complexity
- Query complexity
- Communication complexity
- ...

Quantum-inspired classical algorithms: No exponential speedups is with respect to time and query complexity.

Quantum communication complexity of linear regressions

To explore quantum speedups, we are usually more interested in

- Time complexity
- Query complexity
- Communication complexity
- ...

Quantum-inspired classical algorithms: No exponential speedups is with respect to time and query complexity.

Theorem (Our result, informal)

Quantum computers can have exponential speedups in terms of communication complexity for some fundamental linear algebra problems.

Communication complexity: classical case

Local costs are not considered in communication complexity, and we usually assume Alice and Bob have unlimited computational powers.

The communication can be 1-way or 2-way:

1. 1-way: Only Alice can send information to Bob, or the other way around.
2. 2-way: Alice and Bob can send information to each other.

Communication complexity: quantum case

In the quantum case, Alice and Bob can send quantum states to each other. The complexity is counted by the number of qubits used.

Solving linear regressions: 2-party case

Problem statement.

Alice: $A \in \mathbb{R}^{m \times n}$
Bob: $\mathbf{b} \in \mathbb{R}^m$
Goal: Solve $\arg\min \|A\mathbf{x} - \mathbf{b}\|$

More precisely,

- **in the quantum case: output** $|A^{-1}\mathbf{b}\rangle$ **up to error** ε
- **in the classical case: output samples from a probability distribution** ε**-close to the one defined by** $|A^{-1}\mathbf{b}\rangle$

Solving linear regressions: 2-party case

Problem statement.

Alice: $A \in \mathbb{R}^{m \times n}$
Bob: $\mathbf{b} \in \mathbb{R}^m$
Goal: Solve $\arg\min \|A\mathbf{x} - \mathbf{b}\|$

More precisely,

- **in the quantum case: output $|A^{-1}\mathbf{b}\rangle$ up to error ε**
- **in the classical case: output samples from a probability distribution ε-close to the one defined by $|A^{-1}\mathbf{b}\rangle$**

For simplicity, we assume that the entries of $A, \mathbf{b}$ are specified by $\mathrm{polylog}(mn)$ bits.

Our results

	Alice $\to$ Bob	Bob $\to$ Alice	Alice $\leftrightarrow$ Bob
Q	$\widetilde{O}(\kappa^2 \min(m,n))$	$\widetilde{O}(\kappa^2)$	$\widetilde{O}(\kappa)$
	$\Omega(\min(m,n))$	$\Omega(\kappa^2)$	$\Omega(\kappa)$
C	$\widetilde{O}(mn)$	$\widetilde{O}(m)$	$\widetilde{O}(m)$
	$\Omega(\min(m,n))$	$\Omega(\min(m,n))$	$\Omega(\min(m,n))$
	at most quadratic	can be exponential	can be exponential

$\to$ 1-way communication; $\leftrightarrow$ 2-way communication.

$\kappa =$ condition number of $A \in \mathbb{R}^{m \times n}$.

All lower bounds hold even if $m = n, \kappa = O(1)$.

Quantum protocol (eg): 1-way from Bob to Alice

- Bob sends the state $|0\rangle|\mathbf{b}\rangle$ to Alice.

Quantum protocol (eg): 1-way from Bob to Alice

- Bob sends the state $|0\rangle|\mathbf{b}\rangle$ to Alice.
- Alice constructs a unitary U such that

$$U = \begin{pmatrix} A^{-1}/\|A^{-1}\| & * \\ * & * \end{pmatrix}.$$

She then applies U to $|0\rangle|\mathbf{b}\rangle$:

$$\frac{1}{\|A^{-1}\|}|0\rangle \otimes A^{-1}|\mathbf{b}\rangle + |1\rangle|G\rangle.$$

The success probability is

$$\frac{\|A^{-1}|\mathbf{b}\rangle\|^2}{\|A^{-1}\|^2} \geq \frac{1}{\kappa^2}.$$

Quantum protocol (eg): 1-way from Bob to Alice

- Bob sends the state $|0\rangle|\mathbf{b}\rangle$ to Alice.
- Alice constructs a unitary U such that

$$U = \begin{pmatrix} A^{-1}/\|A^{-1}\| & * \\ * & * \end{pmatrix}.$$

She then applies U to $|0\rangle|\mathbf{b}\rangle$:

$$\frac{1}{\|A^{-1}\|}|0\rangle \otimes A^{-1}|\mathbf{b}\rangle + |1\rangle|G\rangle.$$

The success probability is

$$\frac{\|A^{-1}|\mathbf{b}\rangle\|^2}{\|A^{-1}\|^2} \geq \frac{1}{\kappa^2}.$$

- So Bob has to send $O(\kappa^2)$ copies of $|0\rangle|\mathbf{b}\rangle$ to Alice.

Lower bound analysis

We use the hardness of disjointness problem.

Recall: In this problem, Alice has $(x_1, \ldots, x_n) \in \{0,1\}^n$ and Bob has $(y_1, \ldots, y_n) \in \{0,1\}^n$. They want to determine if $x_i = y_i = 1$ for some i.

[1] Buhrman and de Wolf, Communication complexity lower bounds by polynomials, 2001

[2] Aaronson and Ambainis, Quantum search of spatial regions, 2003.

Lower bound analysis

We use the hardness of disjointness problem.

Recall: In this problem, Alice has $(x_1, \ldots, x_n) \in \{0,1\}^n$ and Bob has $(y_1, \ldots, y_n) \in \{0,1\}^n$. They want to determine if $x_i = y_i = 1$ for some i.

Quantum: $\Theta(n)$ (1-way)[1], $\Theta(\sqrt{n})$ (2-way)[2]
Classical: $\Theta(n)$ (1-, 2-way)

---

[1] Buhrman and de Wolf, Communication complexity lower bounds by polynomials, 2001

[2] Aaronson and Ambainis, Quantum search of spatial regions, 2003.

Lower bound analysis

Alice constructs a diagonal matrix A by

$$A_{ii} = \begin{cases} 1 & x_i = 1, \\ 1/\varepsilon & x_i = 0. \end{cases}$$

Lower bound analysis

Alice constructs a diagonal matrix A by

$$A_{ii} = \begin{cases} 1 & x_i = 1, \\ 1/\varepsilon & x_i = 0. \end{cases}$$

Bob constructs a vector $\mathbf{b}$ by

$$b_i = \begin{cases} 1 & y_i = 1, \\ \varepsilon & y_i = 0. \end{cases}$$

Lower bound analysis

Alice constructs a diagonal matrix A by

$$A_{ii} = \begin{cases} 1 & x_i = 1, \\ 1/\varepsilon & x_i = 0. \end{cases}$$

Bob constructs a vector $\mathbf{b}$ by

$$b_i = \begin{cases} 1 & y_i = 1, \\ \varepsilon & y_i = 0. \end{cases}$$

So the solution of $A\mathbf{x} = \mathbf{b}$ satisfies

$$(A^{-1}\mathbf{b})_i = \begin{cases} 1 & x_i = y_i = 1, \\ \varepsilon & x_i = 1 \text{ xor } y_i = 1, \\ \varepsilon^2 & x_i = y_i = 0. \end{cases}$$

Lower bound analysis

Let

$$P = \{i : x_i = y_i = 1\}, \quad Q = \{i : x_i = 1 \text{ xor } y_i = 1\},$$

then the quantum state of the solution is

$$\frac{1}{\|A^{-1}\mathbf{b}\|}\left(\sum_{i\in P}|i\rangle + \varepsilon\sum_{i\in Q}|i\rangle + \varepsilon^2\sum_{i\notin P\cup Q}|i\rangle\right).$$

Lower bound analysis

Let

$$P = \{i : x_i = y_i = 1\}, \quad Q = \{i : x_i = 1 \text{ xor } y_i = 1\},$$

then the quantum state of the solution is

$$\frac{1}{\|A^{-1}\mathbf{b}\|}\left(\sum_{i\in P}|i\rangle + \varepsilon\sum_{i\in Q}|i\rangle + \varepsilon^2\sum_{i\notin P\cup Q}|i\rangle\right).$$

Choose $\varepsilon = 1/\sqrt{n}$, then

- If $|P| = 1$, the probability of seeing $i \in P$ is as large as a constant ($\approx 1/2$). $\rightarrow$ see the same index many times
- If $|P| = 0$, the state is close to a uniform superposition of indices from Q. $\rightarrow$ see different indices uniformly

Multi-party case

There are s players $P_1, \ldots, P_s$, each P_i has a matrix $A_i \in \mathbb{R}^{m_i \times n}$ and a vector $\mathbf{b}_i \in \mathbb{R}^{m_i}$, they want to solve

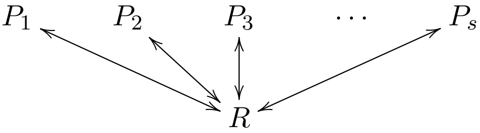
$$\arg\min_{\mathbf{x}} \quad \|A\mathbf{x} - \mathbf{b}\|,$$

where

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_s \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_s \end{pmatrix}.$$

The model we use

Similar to the classical coordinator model, we assume that the communication is 2-way between each player P_i and the referee R, we call this the quantum coordinator model.



Task: the referee outputs

- the quantum state $|A^{-1}\mathbf{b}\rangle \pm \varepsilon$ in the quantum case
- samples from a probability distribution ε-close to the one defined by $|A^{-1}\mathbf{b}\rangle$ in the classical case

The main result

	Upper bound	Lower bound
Quantum	$\widetilde{O}(s^{1.5}\kappa)$	$\Omega(s\kappa)$
Classical	$O(sn^2)$	$\Omega(sn)$

Exponential speedup exists when $s, \kappa \ll n$.

Main technique: Quantum singular value transformation (QSVT).[3]

[3] Gilyén, Su, Low, Wiebe, Quantum singular value transformation, STOC'19

QSVT

Suppose A is Hermitian and there is a unitary

$$U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}.$$

Let $f(x)$ be a bounded polynomial of degree d, then there is a quantum circuit that implements the unitary

$$\widetilde{U} = \begin{pmatrix} f(A/\alpha) & * \\ * & * \end{pmatrix}.$$

It uses $O(d)$ applications of $U, U^\dagger$ and some one- and two-qubit gates.

QSVT

Suppose A is Hermitian and there is a unitary

$$U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}.$$

Let $f(x)$ be a bounded polynomial of degree d, then there is a quantum circuit that implements the unitary

$$\widetilde{U} = \begin{pmatrix} f(A/\alpha) & * \\ * & * \end{pmatrix}.$$

It uses $O(d)$ applications of $U, U^\dagger$ and some one- and two-qubit gates.

$\Rightarrow$ So you can prepare the state $\propto f(A/\alpha)|\psi\rangle$.

QSVT

Theorem (QSVT w.r.t. communication complexity)

In the quantum coordinator model, there is a quantum protocol for the referee to use

$$\widetilde{U} = \begin{pmatrix} f(A/\alpha) & * \\ * & * \end{pmatrix}$$

once with $O(sd \log n)$ *qubits communication.*

Application: linear regression

If $f(x) \approx 1/x$, then we have

Corollary (Linear regression)

There is a quantum protocol for linear regression in cost $\widetilde{O}(s^{1.5}\kappa)$.

[4] Gilyén, Su, Low, Wiebe, Quantum singular value transformation, STOC'19

Application: linear regression

If $f(x) \approx 1/x$, then we have

Corollary (Linear regression)

There is a quantum protocol for linear regression in cost $\widetilde{O}(s^{1.5}\kappa)$.

Recall the time complexity is $\widetilde{O}(T_A \alpha/\sigma_{\min})$,[4] where $\sigma_{\min}$ is the minimal nonzero singular value of A, T_A is the cost of constructing the block-encoding

$$U = \begin{pmatrix} A/\alpha & * \\ * & * \end{pmatrix}.$$

For communication complexity, we can compute $T_A = O(s \log n)$, $\alpha = O(\sqrt{s}\sigma_{\max})$ precisely.

[4] Gilyén, Su, Low, Wiebe, Quantum singular value transformation, STOC'19

Conclusions

QSVT can be dequantized $\rightarrow$ no exponential speedup in terms of time and query complexity for some problems.[5]

[5] Chia et al: 1910.06151; Jethwani, Le Gall, Singh: 1910.05699; Gharibian, Le Gall: 2111.09079

Conclusions

QSVT can be dequantized $\rightarrow$ no exponential speedup in terms of time and query complexity for some problems.[5]

In quantum coordinator model, we can use QSVT $\rightarrow$ efficient quantum communication protocols.

[5] Chia et al: 1910.06151; Jethwani, Le Gall, Singh: 1910.05699; Gharibian, Le Gall: 2111.09079

Conclusions

QSVT can be dequantized → no exponential speedup in terms of time and query complexity for some problems.[5]

In quantum coordinator model, we can use QSVT → efficient quantum communication protocols.

⇒ For many problems where quantum computers lose exponential speedups in terms of time and query complexity, it is possible to have exponential speedups in terms of communication complexity.

[5] Chia et al: 1910.06151; Jethwani, Le Gall, Singh: 1910.05699; Gharibian, Le Gall: 2111.09079

Conclusions

QSVT can be dequantized $\rightarrow$ no exponential speedup in terms of time and query complexity for some problems.[5]

In quantum coordinator model, we can use QSVT $\rightarrow$ efficient quantum communication protocols.

$\Rightarrow$ For many problems where quantum computers lose exponential speedups in terms of time and query complexity, it is possible to have exponential speedups in terms of communication complexity.

$\Rightarrow$ It is interesting to explore more, usually the hard part is the lower bound analysis.

[5] Chia et al: 1910.06151; Jethwani, Le Gall, Singh: 1910.05699; Gharibian, Le Gall: 2111.09079

Conclusions

QSVT can be dequantized $\rightarrow$ no exponential speedup in terms of time and query complexity for some problems.[5]

In quantum coordinator model, we can use QSVT $\rightarrow$ efficient quantum communication protocols.

$\Rightarrow$ For many problems where quantum computers lose exponential speedups in terms of time and query complexity, it is possible to have exponential speedups in terms of communication complexity.

$\Rightarrow$ It is interesting to explore more, usually the hard part is the lower bound analysis.

Thanks very much for your attention!

[5] Chia et al: 1910.06151; Jethwani, Le Gall, Singh: 1910.05699; Gharibian, Le Gall: 2111.09079