Quantum Advantage without Structure[1]

Authors: Takashi Yamakawa & Mark Zhandry (2022)

Manish Kumar

Quantum Tech. (M. Tech) IISc Bengaluru

October 14, 2023

[1] under some assumption

Table of Contents

Table of Contents

Guiding question: Is there a problem with no structure but a verifiable Qauntum advantage?

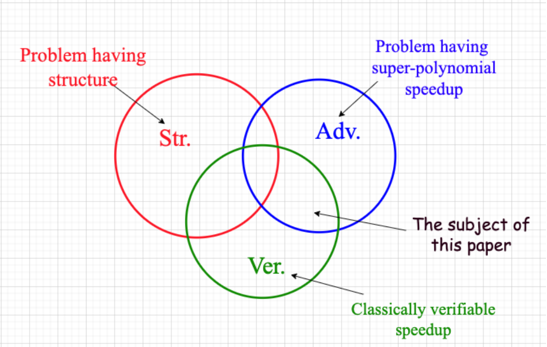

Figure: The set $(\neg Str.) \cap (Adv.) \cap (Ver.)$ is non empty.[2]

[2] As per the claim of the paper

Meaning of Structure-less in this context

Oracle for the problem

- The oracle access (for the problem) is a random oracle.
- Random in the same sense as the randomness of a cryptographic hash function. (Say, SHA2 hash function.)

Theorem:

Relative to a random oracle, there exists an NP serach problem that is solvable by BQP machines but not by BPP machines.

Remark:

- Given the above oracle, the rest remain to come up with a problem that is Quantumly easy but classically hard.
- The paper mentions a contrive(?) case to realize this.

Why Quantumly easy but classically hard?

The exact NP search problem

- Let $C \subseteq \mathbb{F}_q^n$ be a linear code (of a certain type)
- $H_i : \mathbb{F}_q \to \{0, 1\}; i = (1, 2, ..., n)$ be a random oracle
- Find $\mathbf{x} = (x_1, ..x_n)$ such that $\mathbf{x} \in C$ and $H_i(x_i) = 1$

Remark: This is a search problem (over the linear code) rather than a promise/decision problem.

Why it is Quantumly easy task:

An explicit algorithm exists if the linear code is folded Reed-Solomon code

Why it is Classically had task:

There exists (classical) information-theoretic evidence for its hardness (in terms of one ways-ness of such hash function).

Table of Contents

Quantum Algorithm for the problem

Search problem

- Let $C \subseteq \mathbb{F}_q^n$ be a linear code (of a certain type)
- $H_i : \mathbb{F}_q \to \{0,1\}; i = (1,2,...,n)$ be a random oracle
- Find $\mathbf{x} = (x_1, ..x_n)$ such that $\mathbf{x} \in C$ and $H_i(x_i) = 1$

Quantum Algorithm:

Criteria for $\mathbf{x} = (x_1, ..x_n)$ are (i) $\mathbf{x} \in C$ and (ii) $H_i(x_i) = 1$

- **Step I:** Generate $\sum_{\mathbf{x}} V(\mathbf{x}) |\mathbf{x}\rangle$ and $\sum_{\mathbf{x}} W(\mathbf{x}) |\mathbf{x}\rangle$; where $V(\mathbf{x}) = 1$ iff $V(\mathbf{x}) \in C$, and where $W(\mathbf{x}) = 1$ iff $H_i(x_i) = 1$.
- **Step II:** Multiply† above two quantum states to get $\sum_{\mathbf{x}} V(\mathbf{x}) \cdot W(\mathbf{x}) |\mathbf{x}\rangle$.
- **Step III:** Measure the state to get $\mathbf{x}$ that satisfies both the above criteria.

Remark(caveat): Multiplication of two arbitrary states is not always possible.
There are some sufficient requirements to be fulfilled by these quantum states.
For folded Reed-Solomon code, these sufficient conditions are easily met.

Arguments for classical hardness of the problem

Two sufficient condition for classical toughness

Let the linear code $C \subset \Sigma^n$, where Σ is the alphabet.

- If the set of symbols obtained at each position is distinct
- If C is information-theoretic list recoverable

Then oneway-ness is guaranteed with a very high probability.
[due to Haitner et.al (CRYPTO2015)]

Remarks

- The choice of folded Reed-Solomon also has the above two properties
- This particular choice makes the search problem Quantumly easy but classically hard
- This is as per my best understanding

Table of Contents

Conclusions

- Although Oracle is random, the Quantum advantage exists for certain special linear codes.
- In some sense, the structure-less-ness of the oracle is relaxed at the cost of having structure in the coding problem.
- Albeit this specially designed NP search problem is in BQP but outside BPP.

Thank You for Your Attention!