Verifiable Quantum Advantage without Structure

Takashi Yamakawa (NTT Social Informatics Laboratories)
Mark Zhandry (NTT Research & Princeton University)
Can quantum computers offer a superpolynomial computational advantage?
Can such advantage be efficiently **verified**?
Is **structure** needed for quantum advantage?

Current state of complexity theory

$\Rightarrow$ no unconditional results
Option 1: Oracle Separations

Classical algorithms

| \( A \) | \( f(x) \) | \( x \) |

Quantum algorithms

\[
|A\rangle = \sum_{x,y} \alpha_{x,y} |x,y \rangle f(x) \]

no structure = random oracle
Option 2: Conditional Separations

Prove advantage under some computational assumption

Our take: No structure

Structure

Unconditional $P \neq NP$
Symmetric crypto
Public key crypto
Isogenies
Factoring
Discrete log
Pairings
LWE

SKE $\leftrightarrow$ RO $\rightarrow$ classical PKE
[Impagliazzo-Rudich’89]
Verifiable

[Bernstein–Vazirani’92, Simon’94]: $\mathsf{BQP}^A \not\subseteq \mathsf{BPP}^A$

[Shor’94]: Factoring, discrete log

[Hallgren’02]: Pell’s eqns, principal ideal

[Babai-Beals-Seress’09]: Matrix group membership

[Brakerski-Christiano-Mahadev-Vazirani-Vidick’18]: from LWE

Structureless

[Raz-Tal’19]: $\mathsf{BQP}^A \not\subseteq \mathsf{PH}^A$

[Aaronson’09]: Fourier fishing

[Bremner-Jozsa-Shepherd’10, Aaronson-Arkhipov’11]: simulating quantum circuits

This work
All existing oracle-free advantage in NP relies on period-finding

All existing structure-less sources of advantage are sampling problems

[Aaronson-Ambanis’09]: under a plausible conjecture

\[ 0/1 \leftarrow |A\rangle \xrightarrow{\text{q queries}} \text{RO} \xrightarrow{\text{poly}(q)} \approx 0/1 \leftarrow S \]

S potentially computationally unbounded

Basically, random oracles shouldn’t help separating BQP from BPP
This work: verifiable quantum advantage without structure

Results: relative to random oracle with probability 1:

- \( \exists \) NP search problem in BQP \( \setminus \) BPP

- \( \exists \) OWF, CRHFs, signatures that are classically hard but quantumly easy

Assuming classically hard PKE, \( \exists \) PKE that is classically hard but quantumly easy

- \( \exists \) publicly verifiable proof of quantumness with minimal rounds

Under the AA conjecture, \( \exists \) certifiable randomness with minimal rounds

Can replace RO with SHA256 to obtain conjectured non-relativized versions
Our Construction
Random Subset of x-coordinates

Determined by querying random oracle
Random Subset of y-coordinates

Repeat for all coordinates
Questions:

- Why classically hard?
- Why quantumly easy?
- What code to use?
Why/when should it be classically hard?
Domain-constrained Linear Equations

[Ajta’96]: Random linear code + low $L_2$ norm (SIS)

[Applebaum-Haramaty-Ishai-Kushilevitz-Vaikuntanathan’17]

[Yu-Zhang-Weng-Guo-Li’17]: Random binary linear code
+ low Hamming weight

[Brakerski-Lyubashevsky-Vaikuntanathan-Wichs’18]

These seem likely to be (quantum) hard
**Def:** \( \text{Dist}(c, S_1 \times S_2 \times \ldots \times S_n) := \# \{ i : c_i \notin S_i \} / n \)

**Def:** \( C \) is list recoverable if \( \exists \delta, \varepsilon, \varepsilon' \) such that, if \( |S_1|, |S_2|, \ldots, |S_n| \leq 2^{n\varepsilon} \), then

\[
\# \{ c \in C : \text{Dist}(c, S_1 \times S_2 \times \ldots \times S_n) \leq \delta \} \leq 2^{n\varepsilon'}
\]

Examples:
- Folded Reed-Solomon [Guruswami-Rudra’05]
- Random Linear codes [Rudra-Wootters’17]

**Thm:** list recoverable \( \iff \) classically intractable

Concretely, \( \Pr[\text{poly}(n) \ \text{queries give solution}] \leq 2^{n\varepsilon'} \times 2^{-\delta n} \)

[Haitner-Ishai-Omri-Shaltiel’15]:
List recovery \( \rightarrow \) parallel hashing
Why/when should it be quantumly easy?
“Multiplying” quantum states
[Regev’05]
\[
\sum_x \alpha_x |x\rangle \times \sum_x \beta_x |x\rangle = \sum_x \alpha_x \beta_x |x\rangle
\]

Ignoring normalization
Switch to Fourier Domain: Convolution

\[ \sum_x \hat{\alpha}_x |x\rangle \quad * \quad \sum_y \hat{\beta}_y |y\rangle = \sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x + y\rangle \]
1. Construct separately:
\[
\left( \sum_x \hat{\alpha}_x |x\rangle \right) \otimes \left( \sum_y \hat{\beta}_y |y\rangle \right) = \sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y\rangle
\]

2. Add “in superposition”:
\[
\sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y\rangle \rightarrow \sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y, x + y\rangle
\]

3. Decode \( x + y \rightarrow (x, y) \) in reverse:
\[
\sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x, y, x + y\rangle \rightarrow \sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x + y\rangle
\]
* __________ = _______________
Example [Regev’05]:

Primal domain:

\[ \alpha_x = \text{indicator for linear code } C \]

\[ \beta_x \propto e^{-|x|^2 / \sigma^2} \]

Product \( \approx \) short vectors in \( C \)

aka SIS

quantum hardness of SIS

\[ \Rightarrow \]

quantum hardness of LWE

Fourier domain:

\[ \hat{\alpha}_x = \text{indicator for } C^\perp \]

\[ \hat{\beta}_x \propto e^{-|x|^2 / (\sigma')^2} \]

Step 3 \( \approx \) bounded dist. decoding

aka LWE
Applying to our construction
\[ \alpha_x = \text{indicator for } C \]

\[ \beta_x = \text{indicator for valid coordinates} \]

Product = solutions to our problem
What is the decoding problem?
The dual code $C^\perp$
$\beta_x$ for 1 dimension

Complex phase $|\cdot|^2 \approx 1/2$
\[ x + y = \text{(dual codeword)} + \text{(random errors in } \approx \frac{1}{2} \text{ coordinates)} \]

**Thm:** Can decode efficiently \textbf{whp} if \( C^\perp \) is \textbf{list-decodable} for \( \frac{1}{2} + \varepsilon \) fraction of errors

**Good news:** Dual of Folded RS is another Folded RS, has essentially optimal list-decoding
**Challenge:** In general, “whp” decoding not good enough

Actual convolution theorem:

\[
\sum_{x,y} \hat{\alpha}_x \hat{\beta}_y |x + y\rangle \leftrightarrow \sqrt{N} \sum_x \alpha_x \beta_x |x\rangle
\]

Error terms in decoding naively get multiplied by exponential

[Regev’05]: error prob \( \ll N^{-1} \) \( \rightarrow \) still small after multiplying

Our work: error prob \( \gg N^{-1} \) \( \rightarrow \) delicate analysis needed
Applications
1. NP search problem in $\text{BQP} \setminus \text{BPP}$

$$R^O : \{0, 1\}^n \times \Sigma^n \to \{0, 1\}$$

$$R^O (x, w) := \begin{cases} 1 & \text{if } w \in C \land O(i||w_i) = x_i \forall i \\ 0 & \text{otherwise} \end{cases}$$
2. Classical/Quantum Separations for Crypto

\[
\text{OWF}^O : C \rightarrow \{0, 1\}^n
\]

\[
\text{OWF}^O(c) := O(1\|c_1) \parallel O(2\|c_2) \parallel \cdots \parallel O(n\|c_n)
\]
3. Proof of Quantumness
**Def:** Proof of Quantumness

[Brakerski-Christiano-Mahadev-Vazirani-Vidick’18]
Uniform (oracle-independent) adversaries

\[ c \in C : O(i || c_i) = 0 \forall i \]

Oracle-dependent non-uniform adversaries

\[ r \leftarrow \{0, 1\}^n \]

\[ c \in C : O(r || i || c_i) = 0 \forall i \]

**Thm ([Chung-Guo-Liu-Qian’20]):** Salting defeats non-uniformity
4. Certifiable Randomness
Def: Certifiable Randomness
[Brakerski-Christiano-Mahadev-Vazirani-Vidick’18]
Uniform adversaries

\[ c \in C : O(i || c_i) = 0 \forall i \]

Ext \((s, c)\)

**Thm:** AA conjecture \(\Rightarrow\) c has min-entropy
Uniform adversaries

$c \in C : O(i||c_i) = 0 \forall i$

Non-uniform adversaries

$r \leftarrow \{0, 1\}^n$

$c \in C : O(r||i||c_i) = 0 \forall i$

Problem: [Chung-Guo-Liu-Qian’20] naively requires large salts

$\text{Ext}(s, c)$

$\text{Ext}(s, c)$
Is it practical?
Thanks!