Quantum Proofs of Proximity

Marcel Dall'Agnol
University of Warwick

Tom Gur
University of Warwick

Subhayan Roy Moulik
University of Oxford
& UC Berkeley

Justin Thaler
Georgetown University

TQC 2021

Introduction

Part I: Quantum algorithms

Part II: Complexity separations

Introduction

Part I: Quantum algorithms

Part II: Complexity separations

Introduction: $\mathcal{QMA}$

$$P \xrightarrow[|\psi\rangle]{} V$$

Decide language $\mathcal{L}$ in polynomial time, with non-interactive proof.

Introduction: $\mathcal{QMA}$

$$P \xrightarrow[|\psi\rangle]{} V$$

Decide language $\mathcal{L}$ in polynomial time, with non-interactive proof.
Delegation of computation: *prover* computes, *verifier* checks.

$$P \xrightarrow[|\psi\rangle]{} V(x)$$

Given $x \in \{0,1\}^n$ and a poly(n)-qubit state $|\psi\rangle$,

- if $x \in \mathcal{L}$, $\exists\, |\psi\rangle$ such that V accepts w.p. $\geq 2/3$;
- if $x \notin \mathcal{L}$, $\forall\, |\psi\rangle$, V accepts w.p. $\leq 1/3$.

V runs in poly(n) time. [Kitaev et al., 2002]

Introduction: $\mathcal{QMA}$

$$P \xrightarrow[|\psi\rangle]{} V(x)$$

Given $x \in \{0,1\}^n$ and a poly(n)-qubit state $|\psi\rangle$,

- if $x \in \mathcal{L}$, $\exists\,|\psi\rangle$ such that V accepts w.p. $\geq 2/3$;
- if $x \notin \mathcal{L}$, $\forall\,|\psi\rangle$, V accepts w.p. $\leq 1/3$.

V runs in $\tilde{O}(n)$ time.

Introduction: $\mathcal{QMA}$

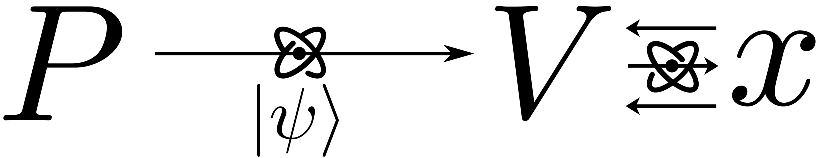
$$P \xrightarrow[|\psi\rangle]{} V(x)$$

Given $x \in \{0,1\}^n$ and a poly(n)-qubit state $|\psi\rangle$,

- if $x \in \mathcal{L}$, $\exists\, |\psi\rangle$ such that V accepts w.p. $\geq 2/3$;
- if $x \notin \mathcal{L}$, $\forall\, |\psi\rangle$, V accepts w.p. $\leq 1/3$.

V runs in $o(n)$ time?

$\mathcal{QMA}$ + property testing

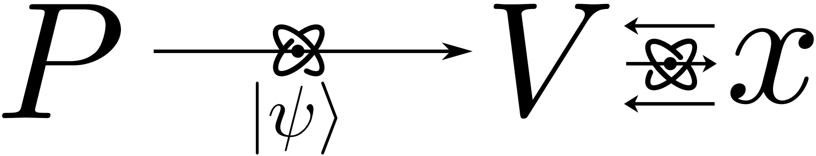


Given quantum query access to $x \in \{0,1\}^n$ and a state $|\psi\rangle$,

- if $x \in \mathcal{L}$, $\exists |\psi\rangle$ such that V accepts w.p. $\geq 2/3$;
- if x is ε-*far* from $\mathcal{L}$, $\forall |\psi\rangle$, V accepts w.p. $\leq 1/3$.

V makes $q = o(n)$ queries and proof has $p = o(n)$ qubits.

$\mathcal{QMA}$ + property testing



Given quantum query access to $x \in \{0,1\}^n$ and a state $|\psi\rangle$,

- if $x \in \Pi$, $\exists\, |\psi\rangle$ such that V accepts w.p. $\geq 2/3$;
- if x is ε-*far* from Π, $\forall\, |\psi\rangle$, V accepts w.p. $\leq 1/3$.

V makes $q = o(n)$ queries and proof has $p = o(n)$ qubits.

$\mathcal{QMAP}(\varepsilon, p, q)$:

properties Π such that…

…given quantum query access to $x \in \{0,1\}^n$ and a state $|\psi\rangle$,

- if $x \in \Pi$, $\exists\, |\psi\rangle$ such that V accepts w.p. $\geq 2/3$;
- if x is ε-far from Π, $\forall\, |\psi\rangle$, V accepts w.p. $\leq 1/3$.

V makes q queries and proof has p qubits.

Introduction

Part I: Quantum algorithms

Part II: Complexity separations

Theorem (Amplitude amplification [Brassard et al., 2002])

If a one-sided randomised algorithm makes q queries and detects an error with probability ρ, there is a quantum algorithm making $O(q/\sqrt{\rho})$ queries that succeeds w. p. $2/3$.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

Classically, we're out of luck: $\Omega(n)$ with any proof.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

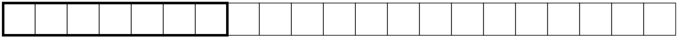
Classically, we're out of luck: $\Omega(n)$ with any proof.
Quantumly, an $n^{2/3}$-bit proof and $O(n^{2/3})$ queries suffice!

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$x =$ 

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$x =$ 

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$x =$ 

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$x =$ 

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$x =$ 

$\pi = \; 1 \;\; 1 \;\; 0$

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$x =$ 

$\pi = \; 1 \; 1 \; 0$

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$$x = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}\hline \; & \; & \; & \; & \; & \; & \; & 1 & 1 & 0 & 0 & 1 & 0 & 0 & \; & \; & \; & \; & \; & \; & \; \\ \hline \end{array}$$

$$\pi = 1 \;\; 1 \;\; 0$$

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Problem: Verify if $x \in \{0,1\}^n$ has even parity.

$$x = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}\hline & & & & & & & & & & & & & \\ \hline \end{array}\boxed{\begin{array}{c|c|c|c|c|c|c} 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}}$$

$$\pi = 1 \;\; 1 \;\; 0$$

If the parity of the proof π is odd, reject.
Sample $i \in [p]$ uniformly and query the i^{th} block of n/p bits. Accept if their parity matches π_i, reject otherwise.

Theorem (Amplitude amplification)

q *queries*	$\Longrightarrow$	$q/\sqrt{\rho}$ *queries*
ρ *detection probability*		$2/3$ *detection probability*

Theorem (Amplitude amplification)

q queries	$\Longrightarrow$	*$q/\sqrt{\rho}$ queries*
ρ detection probability		*2/3 detection probability*

$$\Downarrow$$

Seting $p = n^{2/3}$ in the previous algorithm, it makes $n^{1/3}$ queries to detect an error with probability $1/n^{2/3}$. Therefore,

$$q = O\left(\frac{n^{1/3}}{\sqrt{1/n^{2/3}}}\right) = O(n^{2/3}).$$

Theorem

A similar strategy works for every decomposable property.

Theorem

A similar strategy works for every decomposable property.

Includes:

- k-monotonicity;
- acceptance by branching programs;
- membership in context-free languages;
- Eulerian graph orientations.

Techniques

Decomposable properties: known *classical* proofs of proximity
[Gur and Rothblum, 2018, Goldreich et al., 2018]

Bipartiteness: Quantum collision-finding algorithm
[Ambainis, 2007, Ambainis et al., 2011]

Techniques

Decomposable properties: known *classical* proofs of proximity
[Gur and Rothblum, 2018, Goldreich et al., 2018]

Bipartiteness: Quantum collision-finding algorithm
[Ambainis, 2007, Ambainis et al., 2011]

Techniques

Decomposable properties: known *classical* proofs of proximity
[Gur and Rothblum, 2018, Goldreich et al., 2018]

Bipartiteness: Quantum collision-finding algorithm
[Ambainis, 2007, Ambainis et al., 2011]

Introduction

Part I: Quantum algorithms

Part II: Complexity separations

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{P}$	$\mathcal{NP}$	$\mathcal{IP}$
Quantum			

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$		
Quantum			

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	
Quantum			

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum			

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum			

$\mathcal{C} := \mathcal{C}(\varepsilon, p, q)$ with $p, q = \mathrm{polylog}(n)$ and
ε a small enough constant.

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$		

$\mathcal{C} := \mathcal{C}(\varepsilon, p, q)$ with $p, q = \mathrm{polylog}(n)$ and

ε a small enough constant.

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$	$\mathcal{QMAP}$	

Also $\mathcal{QCMAP}$: $$P \longrightarrow V \rightleftarrows x$$

$\mathcal{C} := \mathcal{C}(\varepsilon, p, q)$ with $p, q = \mathrm{polylog}(n)$ and
ε a small enough constant.

Complexity classes

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$	$\mathcal{QMAP}$	$\mathcal{QIPP}$

Also $\mathcal{QCMAP}$: $$P \longrightarrow V \leftrightarrows x$$

$\mathcal{C} := \mathcal{C}(\varepsilon, p, q)$ with $p, q = \mathrm{polylog}(n)$ and
ε a small enough constant.

Theorem

The following separations hold:

- $\mathcal{QMAP} \not\subseteq \mathcal{MAP} \cup \mathcal{QPT}$, *i.e., quantum input access with a proof are more powerful in tandem than separately;*

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$	$\mathcal{QMAP}$	

Theorem

The following separations hold:

- $\mathcal{QMAP} \not\subseteq \mathcal{MAP} \cup \mathcal{QPT}$, *i.e., quantum input access with a proof are more powerful in tandem than separately;*
- $\mathcal{QMAP} \not\subseteq \mathcal{QCMAP}$, *i.e., classical proofs are weaker than quantum even with a quantum verifier;*

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$	$\mathcal{QMAP}$	

Theorem

The following separations hold:

- $\mathcal{QMAP} \not\subseteq \mathcal{MAP} \cup \mathcal{QPT}$, *i.e., quantum input access with a proof are more powerful in tandem than separately;*
- $\mathcal{QMAP} \not\subseteq \mathcal{QCMAP}$, *i.e., classical proofs are weaker than quantum even with a quantum verifier;*
- $\mathcal{IPP} \not\subseteq \mathcal{QMAP}$, *i.e., quantum proofs cannot substitute for interaction.*

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$	$\mathcal{QMAP}$	

$$\begin{tikzcd}
 & \mathcal{MAP} \arrow[rr] \arrow[ddr] \arrow[dd, shift left, red, "/" marking] & & \mathcal{IPP} \arrow[dd, red, "/" marking] \\
\mathcal{PT} \arrow[ur] \arrow[dr] & & & \\
 & \mathcal{QPT} \arrow[r] \arrow[uu, shift left, red, "/" marking] & \mathcal{QCMAP} \arrow[r, shift left] & \mathcal{QMAP} \arrow[l, shift left, red, "/" marking]
\end{tikzcd}$$

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$	$\mathcal{QMAP}$	

$$
\begin{tikzcd}
 & \mathcal{MAP} \arrow[rr] \arrow[dd, shift left, red, "/" marking] \arrow[ddr] & & \mathcal{IPP} \arrow[dd, "/" marking] \\
\mathcal{PT} \arrow[ur] \arrow[dr] & & & \\
 & \mathcal{QPT} \arrow[uu, shift left, "/" marking] \arrow[r] & \mathcal{QCMAP} \arrow[r, shift left] & \mathcal{QMAP} \arrow[l, shift left, "/" marking]
\end{tikzcd}
$$

	V	$V \leftarrow P$	$V \leftrightarrow P$
Classical	$\mathcal{PT}$	$\mathcal{MAP}$	$\mathcal{IPP}$
Quantum	$\mathcal{QPT}$	$\mathcal{QMAP}$	

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

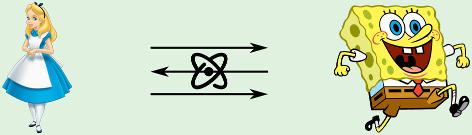
$\mathcal{PT}$ lower bounds via communication complexity have proven very successful. [Blais et al., 2012]

What about $\mathcal{QPT}$? [Montanaro and de Wolf, 2013]

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

$\mathcal{PT}$ lower bounds via communication complexity have proven very successful. [Blais et al., 2012]

What about $\mathcal{QPT}$? [Montanaro and de Wolf, 2013]



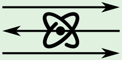
$x \in \{0,1\}^n$ $y \in \{0,1\}^n$

Is there $i \in [n]$ such that $x_i = y_i = 1$?

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

$\mathcal{PT}$ lower bounds via communication complexity have proven very successful. [Blais et al., 2012]

What about $\mathcal{QPT}$? [Montanaro and de Wolf, 2013]



$x \in \{0,1\}^n$ $\qquad\qquad$ $y \in \{0,1\}^n$

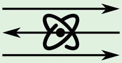
Is there $i \in [n]$ such that $x_i = y_i = 1$?

- $\Omega(n)$ classicaly
- $\Omega(\sqrt{n})$ quantumly

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

$\mathcal{PT}$ lower bounds via communication complexity have proven very successful. [Blais et al., 2012]

What about $\mathcal{QPT}$? [Montanaro and de Wolf, 2013]



$x \in \{0,1\}^n$ $\qquad$ $y \in \{0,1\}^n$

Is there $i \in [n]$ such that $x_i = y_i = 1$?

- $\Omega(n)$ classicaly
- $\Omega(\sqrt{n})$ quantumly
- $O(1)$ with $\log n$ proof

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Q: i_1^{th} bit?

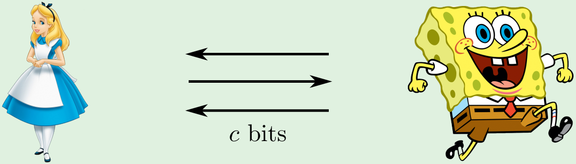
$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Q: i_1^{th} bit?
A: b_1.



$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Q: i_2^{th} bit?

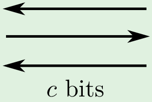
$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Q: i_2^{th} bit?
A: b_2.



$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Q: i_q^{th} bit?

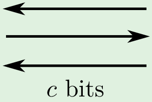
$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we “transfer” communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Q: i_q^{th} bit?
A: b_q.



$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Solving disjointness with $c \cdot q = \Omega(n)$ bits of communication

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

How can we "transfer" communication lower bounds to testers?

Assume there exists property Π such that:

- Π is ε-testable with q queries;
- there exists a mapping C such that $C(x, y) \in \Pi$ if x and y are disjoint, and otherwise $C(x, y)$ is ε-far from Π;
- communicating c bits, we can find out the i^{th} bit of $C(x, y)$.

Solving disjointness with $c \cdot q = \Omega(n)$ bits of communication

$$\Downarrow$$

$$q = \Omega(n/c)$$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C\colon \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B \coloneqq \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C \colon \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B \coloneqq \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C \colon \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B := \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$
$$\Downarrow$$
Quantum ε-tester for B can be used to solve disjointness!

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B \coloneqq \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

$x \in \{0,1\}^n$

$y \in \{0,1\}^n$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B := \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

$x \in \{0,1\}^n$
$\downarrow$
$C(x) \in \{0,1\}^N$

$y \in \{0,1\}^n$
$\downarrow$
$C(y) \in \{0,1\}^N$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B := \{ C(x) : x \in \{0,1\}^n \}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

Goal: simulate a query $|i\rangle |z\rangle \mapsto |i\rangle |z + C(x+y)_i\rangle$

$C(x) \in \{0,1\}^N$

$C(y) \in \{0,1\}^N$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B := \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

Goal: simulate a query $|i\rangle\,|z\rangle \mapsto |i\rangle\,|z + C(x+y)_i\rangle$

$\left(\sum_i |i\rangle\right)|z\rangle$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B \coloneqq \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

Goal: simulate a query $|i\rangle\,|z\rangle \mapsto |i\rangle\,|z + C(x+y)_i\rangle$

$$\left(\sum_i |i\rangle\right)|z\rangle$$
$$\downarrow$$
$$\sum_i |i\rangle|z + C(x)_i\rangle$$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B := \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

Goal: simulate a query $|i\rangle\,|z\rangle \mapsto |i\rangle\,|z + C(x+y)_i\rangle$

$\sum_i |i\rangle|z + C(x)_i\rangle$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B \coloneqq \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

Goal: simulate a query $|i\rangle\,|z\rangle \mapsto |i\rangle\,|z + C(x+y)_i\rangle$

$$\sum_i |i\rangle|z + C(x)_i\rangle$$

$$\downarrow$$

$$\sum_i |i\rangle|z + C(x)_i + C(y)_i\rangle$$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B := \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

Goal: simulate a query $|i\rangle\,|z\rangle \mapsto |i\rangle\,|z + C(x+y)_i\rangle$

$$\sum_i |i\rangle|z + C(x)_i\rangle$$
$$\downarrow$$
$$\sum_i |i\rangle|z + C(x+y)_i\rangle$$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Let $C : \mathbb{F}^n \mapsto \mathbb{F}^N$ be a *linear code* with distance ε.
$B := \{\, C(x) : x \in \{0,1\}^n \,\}$ are the encodings of Boolean messages.

$$x \text{ and } y \text{ are disjoint} \iff C(x+y) \in B$$

Goal: simulate a query $|i\rangle\,|z\rangle \mapsto |i\rangle\,|z + C(x+y)_i\rangle$

$\sum_i |i\rangle|z + C(x+y)_i\rangle$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Each query is simulated by $O(\log N)$ qubits of communication.

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Quantum ε-tester for B with q queries

$\Downarrow$

Protocol with $O(q \log N)$ communication complexity

C locally testable and relaxed locally decodable with $N = n^{1.001}$, [Ben-Sasson et al., 2006]

- $C \setminus B \notin \mathcal{QPT}(\varepsilon, n^{0.49})$

$\mathcal{MAP} \not\subseteq \mathcal{QPT}$: disjointness + relaxed LDC

Quantum ε-tester for B with q queries

$$\Downarrow$$

Protocol with $O(q \log N)$ communication complexity

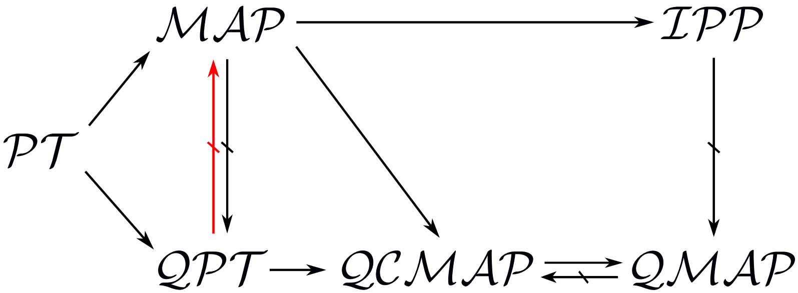
C locally testable and relaxed locally decodable with $N = n^{1.001}$, [Ben-Sasson et al., 2006]

- $C \setminus B \notin \mathcal{QPT}(\varepsilon, n^{0.49})$
- $C \setminus B \in \mathcal{MAP}(\varepsilon, \log n, O(1))$

(Proof points to non-Boolean $i \in [n]$; verifier tests membership in C then decodes i^{th} coordinate and checks if it is Boolean.)

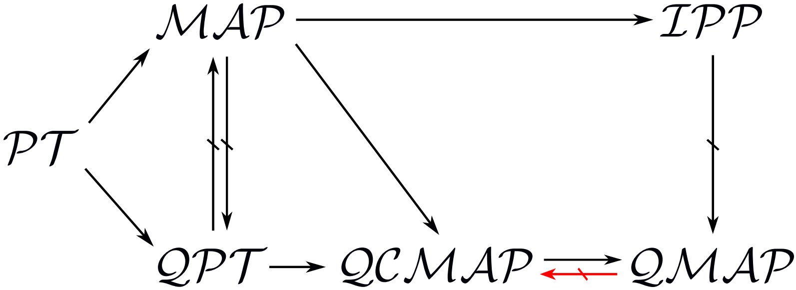
Other separations

$\mathcal{QPT} \not\subseteq \mathcal{MAP}$: Forrelation [Aaronson and Ambainis, 2018]



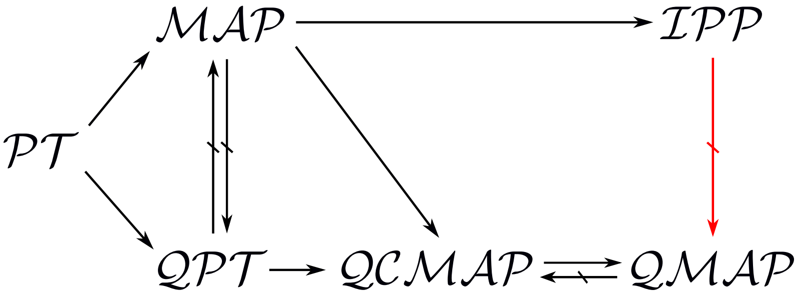
Other separations

$\mathcal{QPT} \not\subseteq \mathcal{MAP}$: Forrelation [Aaronson and Ambainis, 2018]
$\mathcal{QMAP} \not\subseteq \mathcal{QCMAP}$: recasting $\mathcal{QMA} \not\subseteq \mathcal{QCMA}$
[Aaronson and Kuperberg, 2007]



Other separations

$\mathcal{QPT} \not\subseteq \mathcal{MAP}$: Forrelation [Aaronson and Ambainis, 2018]
$\mathcal{QMAP} \not\subseteq \mathcal{QCMAP}$: recasting $\mathcal{QMA} \not\subseteq \mathcal{QCMA}$ [Aaronson and Kuperberg, 2007]
$\mathcal{IPP} \not\subseteq \mathcal{QMAP}$: permutation testing [Gur et al., 2018, Sherstov and Thaler, 2019]



Open problems

- What about $\mathcal{QIPP}$?

Open problems

- What about $\mathcal{QIPP}$?
- Can QIPPs test $\mathcal{NC}$ languages with $o(\sqrt{n})$ proof and query complexities? [Rothblum and Rothblum, 2020]

Open problems

- What about $\mathcal{QIPP}$?
- Can QIPPs test $\mathcal{NC}$ languages with $o(\sqrt{n})$ proof and query complexities? [Rothblum and Rothblum, 2020]

Thank you!

References I

Aaronson, S. and Ambainis, A. (2018).
Forrelation: A problem that optimally separates quantum from classical computing.
SIAM Journal on Computing, 47(3):982–1038.

Aaronson, S. and Kuperberg, G. (2007).
Quantum versus classical proofs and advice.
In *22nd Annual IEEE Conference on Computational Complexity (CCC 2007), 13-16 June 2007, San Diego, California, USA*, pages 115–128. IEEE Computer Society.

Ambainis, A. (2007).
Quantum walk algorithm for element distinctness.
SIAM Journal on Computing, 37(1):210–239.

Ambainis, A., Childs, A. M., and Liu, Y.-K. (2011).
Quantum property testing for bounded-degree graphs.
In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 365–376, Berlin, Heidelberg. Springer Berlin Heidelberg.

Ben-Sasson, E., Goldreich, O., Harsha, P., Sudan, M., and Vadhan, S. (2006).
Robust pcps of proximity, shorter pcps, and applications to coding.
SIAM Journal on Computing, 36(4):889–974.

Blais, E., Brody, J., and Matulef, K. (2012).
Property testing lower bounds via communication complexity.
computational complexity, 21(2):311–358.

Brassard, G., Hoyer, P., Mosca, M., and Tapp, A. (2002).
Quantum amplitude amplification and estimation.
Contemporary Mathematics, 305:53–74.

References II

Goldreich, O., Gur, T., and Rothblum, R. D. (2018).
Proofs of proximity for context-free languages and read-once branching programs.
Information and Computation, 261:175–201.

Gur, T., Liu, Y. P., and Rothblum, R. D. (2018).
An exponential separation between MA and AM proofs of proximity.
In *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Gur, T. and Rothblum, R. D. (2018).
Non-interactive proofs of proximity.
computational complexity, 27(1):99–207.

Kitaev, A. Y., Shen, A. H., and Vyalyi, M. N. (2002).
Classical and Quantum Computation, volume 47 of *Graduate studies in mathematics*.
American Mathematical Society.

Montanaro, A. and de Wolf, R. (2013).
A survey of quantum property testing.
arXiv:1310.2035.

Rothblum, G. N. and Rothblum, R. D. (2020).
Batch verification and proofs of proximity with polylog overhead.
In *Theory of Cryptography Conference*, pages 108–138. Springer.

Sherstov, A. A. and Thaler, J. (2019).
Vanishing-error approximate degree and QMA complexity.
arXiv:1909.07498.

References III

Images:

Server Icon by Rank Sol on Iconscout
Mobile by Momento Design from the Noun Project
Laptop Icon by Jemis Mali from Iconscout
Smartwatch by juan manjarrez from the Noun Project
database by mardjoe from the Noun Project
atom by Fengquan Li from the Noun Project

https://disney.fandom.com/wiki/Alice/Gallery?file=Alice_Render.png

https://loathsomecharacters.miraheze.org/wiki/File:SpongeBob_SquarePants.png