QMA AND THE POWER OF "POSITIVITY"

Kunal Marwaha

University of Chicago

joint with Roozbeh Bassirian, Bill Fefferman (arXiv)

see also Jeronimo and Wu (STOC '23)

QMA AND THE POWER OF "POSITIVITY"

Kunal Marwaha

University of Chicago

joint with Roozbeh Bassirian, Bill Fefferman (arXiv)

see also Jeronimo and Wu (STOC '23)

OUTLINE

1. An introduction to QMA^+
2. Proof outline

OUTLINE

1. **An introduction to QMA^+**
2. Proof outline

CONTEXT: QMA AND $\mathrm{QMA}(2)$

What is the power of *unentangled* proofs?

REVIEW: $\mathrm{QMA}_{c,s}$

Set of decision problems such that:

- If YES (completeness): $\exists\,\mathrm{poly}(n)$-qubit $|\psi\rangle$ input to BQP machine, accepts w.p. $\geq c(n)$.
- If NO (soundness): $\forall\,\mathrm{poly}(n)$-qubit $|\psi\rangle$ input to BQP machine, accepts w.p. $\leq s(n)$.

REVIEW: $\mathrm{QMA}(2)_{c,s}$

Set of decision problems such that:

- If YES (completeness): $\exists \, \mathrm{poly}(n)$-qubit $|\psi_1\rangle \otimes |\psi_2\rangle$ input to BQP machine, accepts w.p. $\geq c(n)$.
- If NO (soundness): $\forall \, \mathrm{poly}(n)$-qubit $|\psi_1\rangle \otimes |\psi_2\rangle$ input to BQP machine, accepts w.p. $\leq s(n)$.

FACTS ABOUT QMA, $\mathrm{QMA}(2)$

Gap amplification (as long as $c(n) - s(n) \geq \frac{1}{\mathrm{poly}(n)}$):

- QMA: via parallel repetition
- $\mathrm{QMA}(2)$: using the *product test* [HM10]

Upper bounds (better than NEXP):

- $\mathrm{QMA} \subseteq \mathrm{PSPACE}$ using semidefinite programming (in fact, $\subseteq \mathrm{PP}$ by Kitaev and Watrous)
- Only $\mathrm{QMA}(2) \subseteq \mathrm{NEXP}$. *Why can't we do better?*

[JW23]: $\mathrm{QMA}^{+}_{c,s}$

Set of decision problems such that:

- If YES (completeness): $\exists\ \mathrm{poly}(n)$-qubit $|\psi\rangle$ **with non-negative amplitudes** input to BQP machine, accepts w.p. $\geq c(n)$.
- If NO (soundness): $\forall\ \mathrm{poly}(n)$-qubit $|\psi\rangle$ **with non-negative amplitudes** input to BQP machine, accepts w.p. $\leq s(n)$.

[JW23]: $\mathrm{QMA}^+(2)_{c,s}$

Set of decision problems such that:

- If YES (completeness): $\exists\ \mathrm{poly}(n)$-qubit $|\psi_1\rangle \otimes |\psi_2\rangle$ **with non-negative amplitudes** input to BQP machine, accepts w.p. $\geq c(n)$.
- If NO (soundness): $\forall\ \mathrm{poly}(n)$-qubit $|\psi_1\rangle \otimes |\psi_2\rangle$ **with non-negative amplitudes** input to BQP machine, accepts w.p. $\leq s(n)$.

HAVEN'T I SEEN THIS BEFORE?

[GKS14] show that $\mathrm{SQMA} = \mathrm{QMA}$,
where we restrict to *subset states* **only in completeness**.

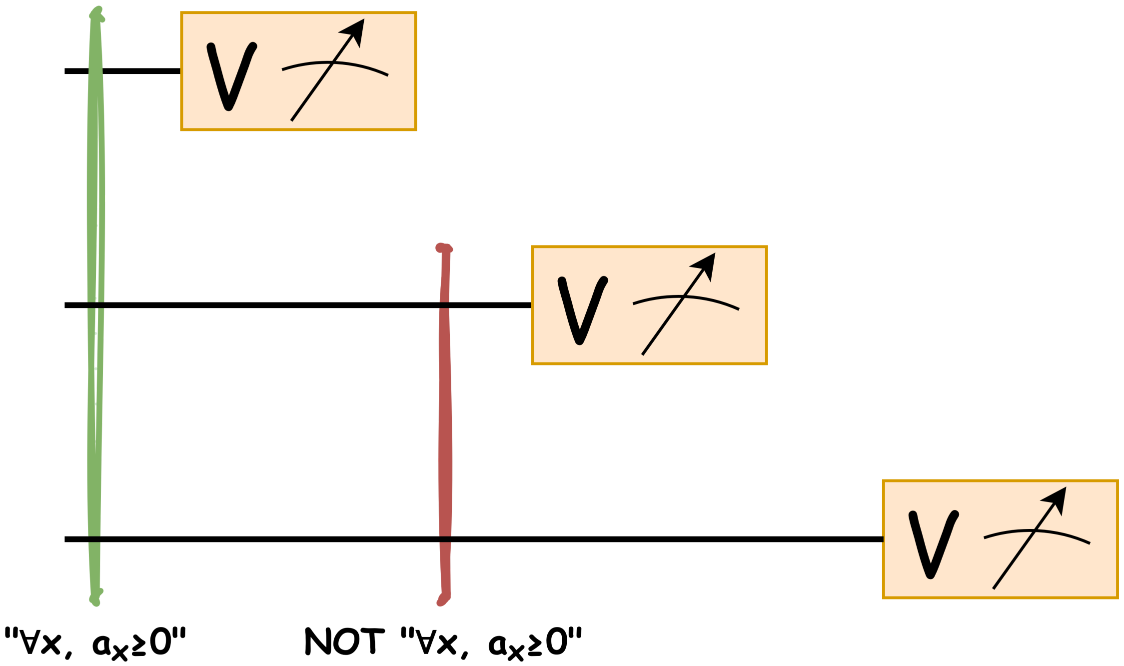
Lesson: Promise-symmetric restrictions can increase power, since they *restrict* Merlin's cheating in soundness.

"FACTS" ABOUT $\mathrm{QMA}^+, \mathrm{QMA}^+(2)$

Gap amplification:

Parallel repetition **fails**.

Reason: Partial measurements can reintroduce complex phases into remaining state.



"FACTS" ABOUT $\mathrm{QMA}^+, \mathrm{QMA}^+(2)$

Upper bounds (better than NEXP):

Using a semidefinite program **fails**.

Reason: Copositive programming is hard!

Optimizing $\max_{x \geq 0} x^\dagger A x$ can compute independence numbers of graphs, etc.

HOW POWERFUL IS THE $(^{+})$?

Every state $|\psi\rangle$ has $\frac{1}{4}$ overlap with some state with non-negative amplitudes.

$\implies$ $\exists$ constants $1 > c' > s' > 0$ s.t. $\mathrm{QMA}^{+}_{c',s'} = \mathrm{QMA}$ and $\mathrm{QMA}^{+}(2)_{c',s'} = \mathrm{QMA}(2)$.

[JW23]: ON $\mathrm{QMA}^+(2)$

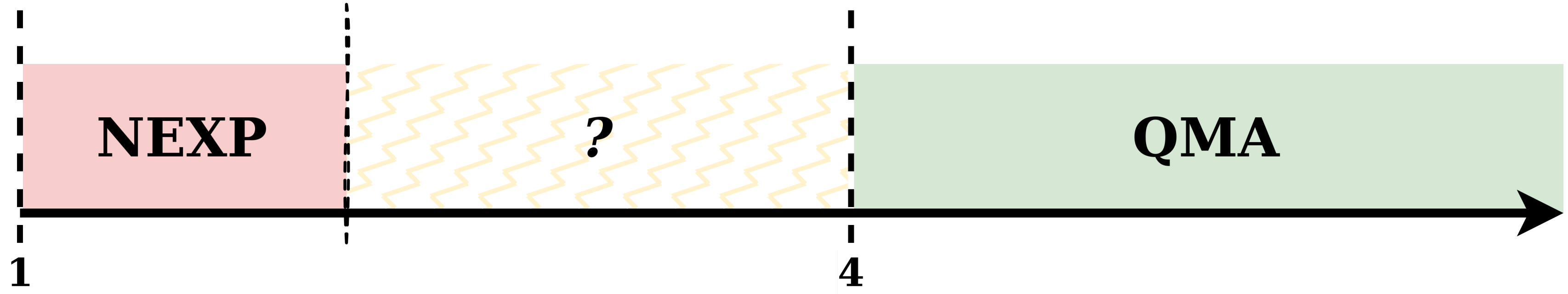
$\exists$ *other* constants $1 > c > s > 0$, s.t.
$\mathrm{QMA}^+(2)_{c,s} = \mathrm{NEXP}$.

New way to understand $\mathrm{QMA}(2)$:
$\mathrm{QMA}^+(2)$ gap amplification $\implies \mathrm{QMA}(2) = \mathrm{NEXP}$!

OUR WORK: ON QMA^+

$\exists$ *other* constants $1 > c > s > 0$, s.t.

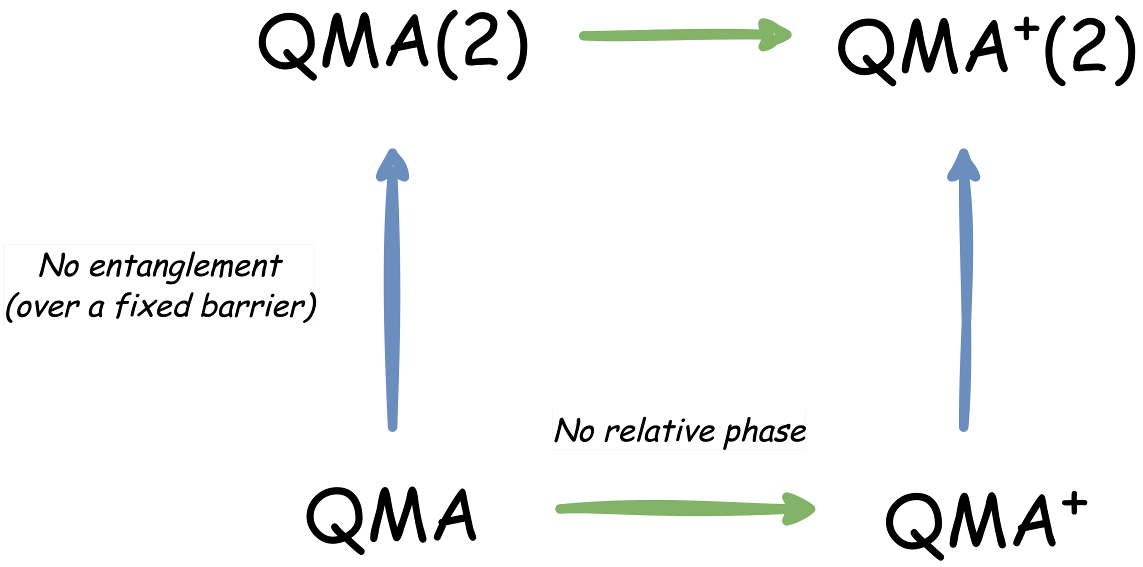
$$\mathrm{QMA}^+_{c,s} = \mathrm{NEXP}!$$



($\frac{c}{s}$ interpolates from QMA to NEXP)

NO gap amplification of QMA^+!

INTERPRETING THESE RESULTS



"Perhaps the power lies in the $^+$*, not the* (2)*..."*

Any technique to amplify the promise gap in $\mathrm{QMA}^+(2)$ must **fail** for QMA^+.

OUTLINE

1. An introduction to QMA^+
2. **Proof outline**

OUTLINE

1. An introduction to QMA^+
2. Proof outline:
    - $\mathrm{NP} \subseteq \mathrm{QMA}^+$ **with $O(\log n)$-qubit proof**
    - Scaling up to $\mathrm{NEXP} \subseteq \mathrm{QMA}^+$

CHOOSING A NP-HARD PROBLEM

Input: CSP instance (n variables, bounded alphabet Σ, q-uniform constraints $\{\mathcal{C}_1, \ldots, \mathcal{C}_R\}$)

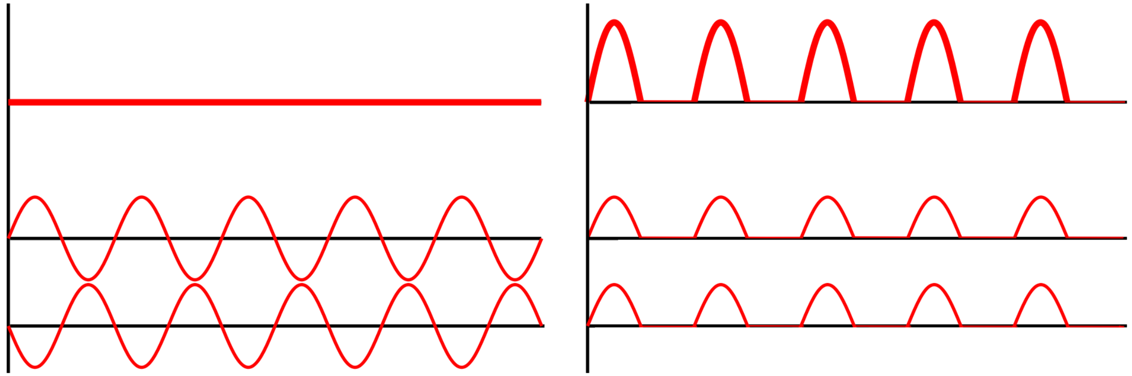
Output: Is instance fully satisfiable (for some $x \in \Sigma^n$)?

PCP Theorem: NP-hard for $q = O(1)$, with completeness $c = 1$ and soundness $s = \frac{1}{2}$ (i.e. *constant* gap).

Plan: Solve this in QMA^+ with $O(\log n)$-sized proof.

AMPLITUDE AND INTERFERENCE

edited from Wikipedia



Intuition: **non-negative amplitudes** "take the interference" out of $|\psi\rangle$ (they don't "cancel out"!)

THE POWER OF PLUS $(^+)$

Goal: *require* Merlin to send a certain type of state.

Big idea of [JW23]: $\langle\psi|+\rangle \propto \||\psi\rangle\|_1$.

$(\Pi_+ := |+\rangle\langle+|$ accepts $|\psi\rangle$ according to its ℓ_1 norm)

This is the **only use** of the $(^+)$ assumption in both papers.

[JW23]'S USE OF $(^{+})$

1. Notice that $\mathrm{QMA}^+(2) = \mathrm{QMA}^+(k)$ by [HM10] (so we can assume many copies of $|\psi\rangle$).
2. Project $\Pi_+|\psi\rangle$ on each copy; count the fraction that accept. (This *estimates* the ℓ_1 norm of $|\psi\rangle$)

$\longrightarrow$ check closeness to states of a *target* ℓ_1 norm.

OUR USE OF $(^+)$

Consider two registers:
question $(\log n$ qubits) and *answer* $(O(1)$ qubits)

We choose one of two tests:

1. $\Pi_+ \otimes \Pi_+$: (dense as possible)
2. $\mathbb{I} \otimes (\mathbb{I} - \Pi_+)$

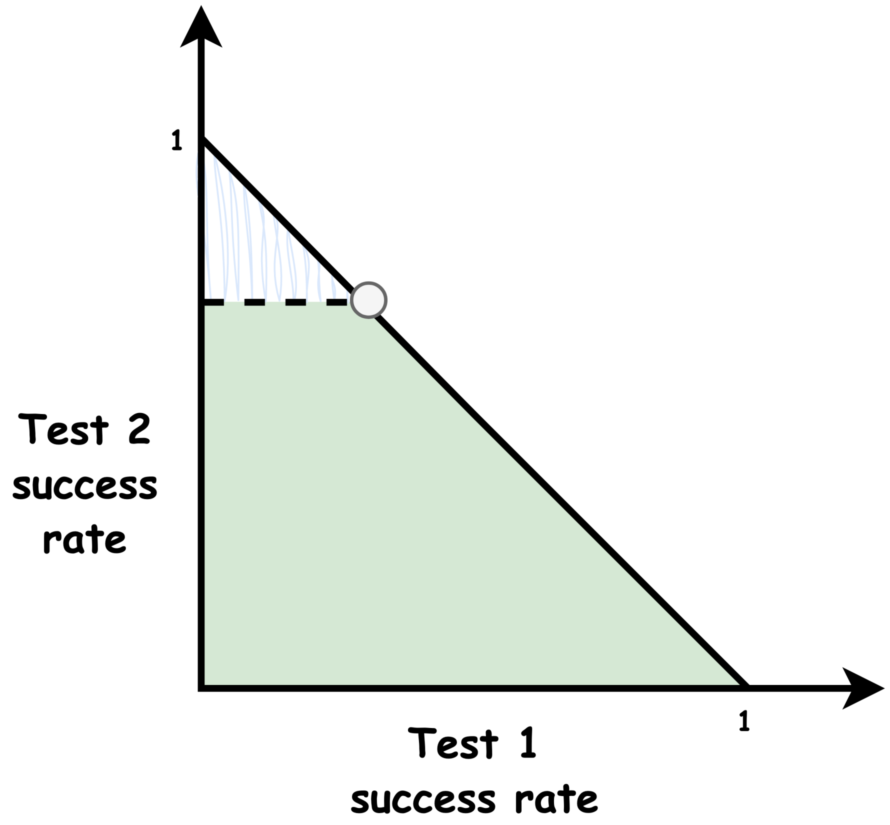
States with **non-negative amplitudes** can't perfectly pass Test 2. The best have *one answer per question*.

$\longrightarrow$ check closeness to states of a *rigid* form:

$$\frac{1}{\sqrt{n}} \sum_{j=1}^{n} |j\rangle|f(j)\rangle$$

OUR USE OF $({}^{+})$

concept: Bryan O'Gorman



- Tests are orthogonal, so sum of success rates ≤ 1.
- Non-negative amplitude states live in green region.
- *Rigid* states at the circled point.

HOW CAN WE USE THIS POWER?

questions $\to$ constraints

answers $\to$ assignments of associated variables

In completeness, $\exists$ satisfying assignment $f : [R] \to \Sigma^q$ and proof $|\psi\rangle := \frac{1}{\sqrt{R}} \sum_{j=1}^{R} |j\rangle|f(j)\rangle$.

With some probability, we test for this *rigid* form.

Otherwise, we check the *constraints* $\{\mathcal{C}_j\}$.

TESTING THE CONSTRAINTS

For *rigid* states, checking the constraints is easy: *measure in computational basis, and test* $\mathcal{C}_j(f(j))$.

But Merlin can cheat: sending different values for the same variable depending on the constraint.

So (with some probability), need to check for *consistency*.

CHECKING "CONSISTENCY"

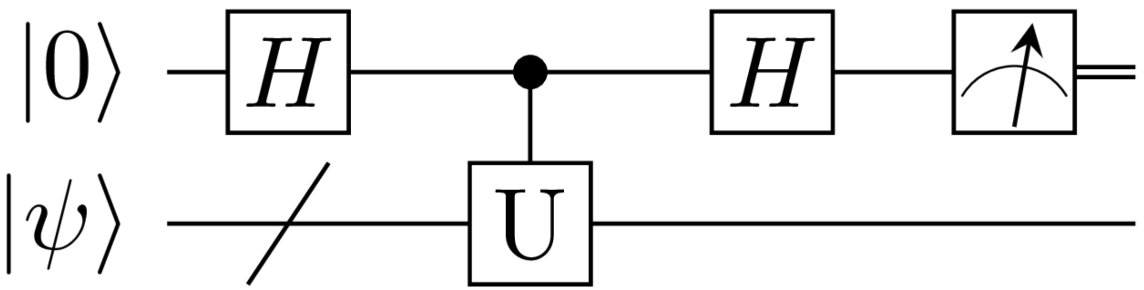
Goal: Construct unitaries $\{U_1, \ldots, U_d\}$ such that:

- Honest: $|\psi\rangle = U_k|\psi\rangle$ for all k
- Cheating: $|\psi\rangle$ "far" from $U_k|\psi\rangle$ for some k

Then, the consistency protocol would:

1. Choose uniform $k \in \{1, \ldots, d\}$
2. Run "Hadamard test" on $(|\psi\rangle, U_k|\psi\rangle)$

source: Victory Omole

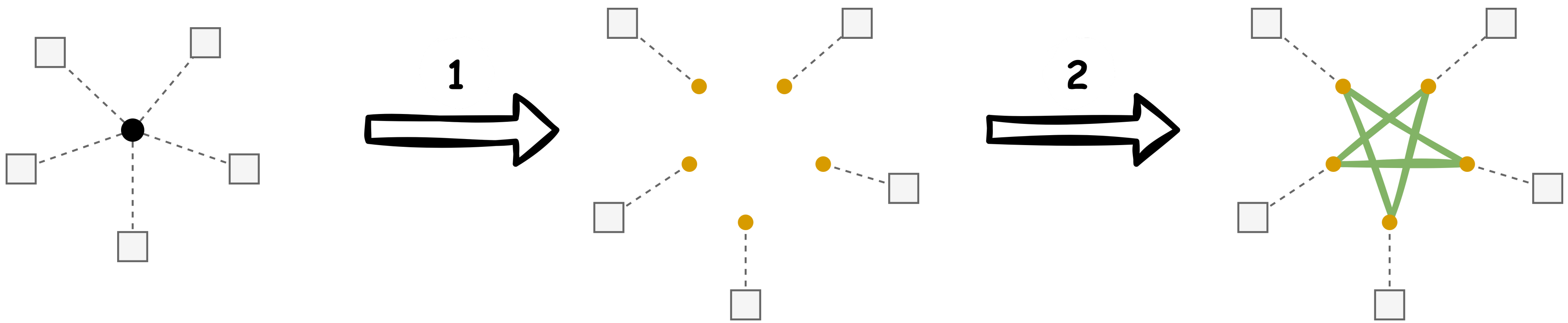


THE "CONSISTENCY" UNITARIES

We build the graph G using a step from [Dinur07]:

1. Turn each variable $i \in [n]$ into a *cluster* of vertices.
   (One vertex ● per constraint ■ involving i.)
2. Add a d-regular *expander* graph ✯ within each cluster.

Illustration for one variable ● and $d = 2$:



G is the *union* of all expander graphs ($R \cdot q$ vertices).

THE “CONSISTENCY” UNITARIES

Recall that a *rigid* state is of the form

$$|\psi\rangle := \frac{1}{\sqrt{R}} \sum_{j=1}^{R} |j\rangle |f(j)\rangle.$$

It is convenient to separate the variable assignments:

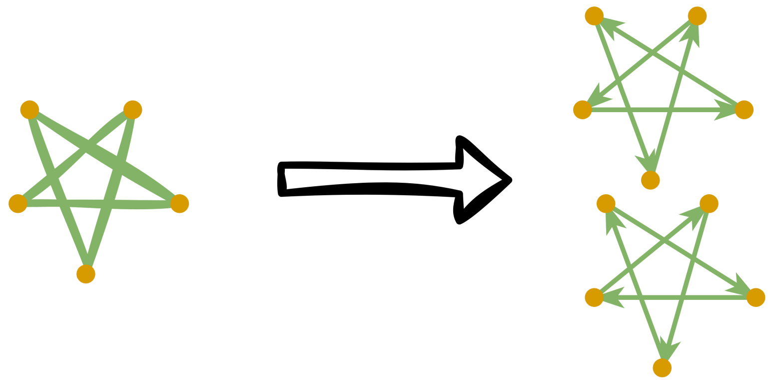
$$|\phi\rangle := \frac{1}{\sqrt{R \cdot q}} \sum_{j=1}^{R} \sum_{\iota=1}^{q} |j, \iota\rangle |f(j)[\iota]\rangle.$$

(Then all vertices of G are in superposition!)

The map $|\psi\rangle \mapsto |\phi\rangle$ is efficient; see paper for details.

THE “CONSISTENCY” UNITARIES

We can always decompose a d-regular graph into d permutations $\{\pi_1, \ldots, \pi_d\}$.



For $k \in [d]$, let $U_k : |j, \iota\rangle|value\rangle \mapsto |\pi_k(j, \iota)\rangle|value\rangle$ for each constraint $j \in [R]$ and variable index $\iota \in [q]$.

Honest assignment $\implies$ $|\phi\rangle = U_k|\phi\rangle$ for all k!

OUTLINE

1. An introduction to QMA^+
2. Proof outline:
   - $\mathrm{NP} \subseteq \mathrm{QMA}^+$ with $O(\log n)$-qubit proof
   - **Scaling up to $\mathrm{NEXP} \subseteq \mathrm{QMA}^+$**

A NEXP-HARD PROBLEM

Input: *Succinct* CSP instance ($N := 2^n$ variables, bounded alphabet Σ, q-uniform constraints $\{\mathcal{C}_1, \ldots, \mathcal{C}_R\}$)

Output: Is instance fully satisfiable (for some $x \in \Sigma^{2^n}$)?

PCP Theorem: NEXP-hard for $q = O(1)$, completeness $c = 1$ and soundness $s = \frac{1}{2}$ (i.e. *constant* gap).

Plan: Solve this in QMA^+ with $O(\mathrm{poly}(n))$-sized proof.

THE NP PROTOCOL *ALMOST* WORKS

Arthur’s protocol needs to be *efficient*.

Only issue: how to do “consistency” test?

- expanders are exponentially large
- could be exponentially many expanders
- adjacency lists could be exponentially large

SOLUTIONS ([JW23])

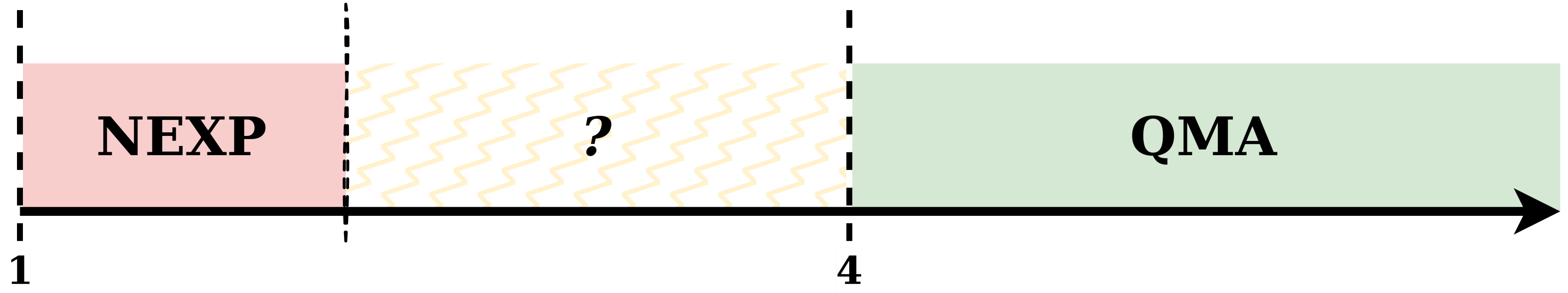
- expanders are exponentially large
  Doubly explicit expander constructions, to build the expanders and decompose them in $\text{polylog}(N)$ time.
- could be exponentially many expanders
  Use a $O(1)$-*strongly uniform* PCP.
- adjacency lists could be exponentially large
  Use a $\text{polylog}(N)$-*doubly explicit* PCP.

Everything else works after making these adjustments! 😎

CONCLUSIONS

Promise-symmetric classes can be very powerful.

But the promise gap *really matters*: $\mathrm{QMA}^{+}_{c,s}$ interpolates from QMA to NEXP for **constant** c, s.



(x-axis: $\frac{c}{s}$)

Is there a phase transition in constants?

CONCLUSIONS

Suppose you use $\mathrm{QMA}^+(2)$ to study $\mathrm{QMA}(2)$...

Any technique to amplify the promise gap in $\mathrm{QMA}^+(2)$ must **fail** for QMA^+.

What does $\mathrm{QMA}^+(2)$ have that QMA^+ doesn't have?

THANK YOU

Kunal Marwaha

https://kunalmarwaha.com/about
kmarw@uchicago.edu

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE-1746045. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.