quantum search-to-decision and state synthesis

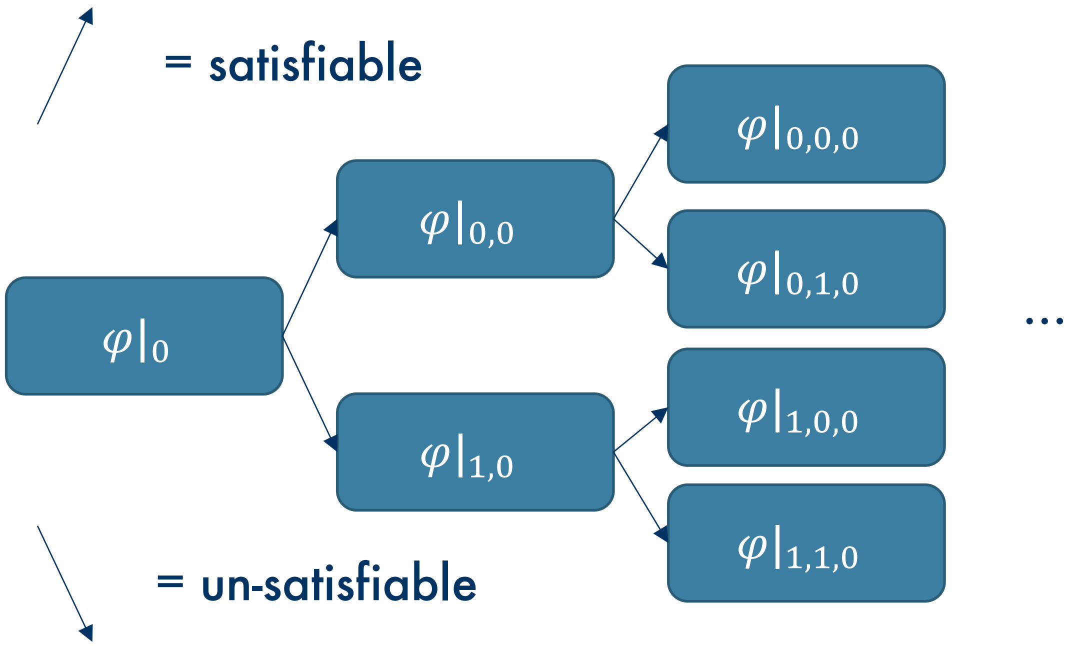
Chinmay Nirkhe (IBM Quantum & UC Berkeley)
Sandy Irani (UC Irvine), Anand Natarajan (MIT),
Sujit Rao (MIT), Henry Yuen (Columbia)

NP has search-to-decision reductions …

- Say there is a black box which takes as input 3SAT formulas φ and outputs (with pr = 1) if they are satisfiable or not
- Crucially, does not tell you the solution (satisfying assignment) $x \in \{0,1\}^n$ s.t. $\varphi(x) = 1$
- This is a black box for NP and repeated uses can be used to build a solution $x \in \{0,1\}^n$

NP has search-to-decision reductions …

- Let $\varphi|_{a_1,a_2,\ldots,a_k}$ be the restriction of φ on the first k variables



After n queries, we learn a complete satisfying assignment.

Does not require randomness.

$$\mathrm{SearchNP} \subseteq \mathrm{P}^{\mathrm{DecisionNP}}$$

Does QMA have search-to-decision?

- In classical CS theory, defining decision problems as the *de facto* model of computation is justified by search-to-decision reductions
- What about in quantum CS? Is the same definition justified? Or do we need to rectify our *de facto* notion of computation?
- **Theorem 1**: QMA-search is reducible to 1-query PP-decision
- **Theorem 2**: Oracle proof that QMA-search not reducible to QMA-decision

Does QMA have search-to-decision?

- BQP algorithm + oracle access to a classical function $f:\{0,1\}^n \to \{0,1\}$
$$|z\rangle \mapsto (-1)^{f(z)}|z\rangle$$
- Given input (H, a, b), produce a state $|\psi\rangle$ so there exists some family of BQP verifiers V s.t.
$$\Pr[V(H, a, b, \psi) = 1] > 0.99 \text{ iff } (H, a, b) \in L_{yes}$$
$$\Pr[V(H, a, b, \psi) = 1] < 0.01 \text{ iff } (H, a, b) \in L_{no}$$
- QMA oracle function f answers correctly if $z \in L_{yes} \cup L_{no}$ but can answer whatever for instances outside promise

Starting point: State synthesis algorithms

- Given a state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ how many oracle queries to a classical function f does it take to synthesize up to ℓ_1-norm $1/\mathrm{poly}(n)$?
- Simple algorithm [Aaronson] gives us a $O(n)$ query algorithm where the complexity of the function f is unbounded.
- Can we do better? Can we do even better when the state is "physically relevant" – i.e. solution to QMA problem?

Starting point: State synthesis algorithms

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} e^{i\theta_x}\sqrt{\Pr[X=x]}\,|x\rangle$$

Step 1: Synthesize $\sum_x \sqrt{\Pr[X=x]}\,|x\rangle$. This is equivalent to coherently synthesizing a sample from dist. X. Can do this with $2n$ oracle queries: build conditional distribution on bit 1. Then conditionally, sample bit 2 and 3 etc until sample is generated.

Step 2: with 2 more queries, apply $|x\rangle \mapsto e^{i\theta_x}|x\rangle$ phase map.

Our improvements on state synthesis

Complexity class	1 query	2 queries	$O(n)$ queries
NP	NP **oracle, $\Omega(n^{-1})$ success probability, Theorem 2.7**	$\leftarrow$	NP oracle, classical queries (folklore)
QCMA	QCMA **oracle, $\Omega(n^{-1})$ success probability, Theorem 2.7**	$\leftarrow$	QCMA oracle, classical queries (folklore)
QMA	PP **oracle,** $1/\text{poly}(n)$ **precision, Theorem 1.1**	$\leftarrow$ (Theorem 1.4 applies but is time-inefficient)	PP oracle, $1/\exp(n)$ precision [Aar16]
QMA_{exp} (= PSPACE)	PSPACE **oracle** $\Omega(1)$ **overlap, Theorem 1.1**	$\leftarrow$ (Theorem 1.4 applies but is time-inefficient)	PSPACE oracle, $1/\exp(n)$ precision [Aar16]
Arbitrary states	**Arbitrary oracle,** $1/\text{poly}(n)$ **precision, Theorem 1.3**	**Arbitrary oracle,** $1/\exp(n)$ **precision, 2 queries, Theorem 1.4**	Arbitrary oracle, $1/\exp(n)$ precision [Aar16]

1-query state synthesis for QMA

Thm 1: Let (H, a, b) be a local Hamiltonian problem. If the problem is a yes instance, there exists a BQP algorithm making 1-query to a PP-oracle s.t. the output state of the algorithm has energy $\leq a + (b - a)/2$.

note: the complexity of the prev. state synthesis algorithm was also PP (but with $2n + 2$ *queries).*

Interlude: Phase states

Let $f:\{0,1\}^n \to \{0,1\}$ be any boolean function. Phase state:

$$|\psi_f\rangle = \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle$$

There are 2^{2^n} phase states. For any given state $|\tau\rangle$, a decent estimator of $|\tau\rangle$ is $f(x) = \operatorname{sgn}\Re(\langle x|\tau\rangle)$. In the sense that whp for Haar-random τ,

$$\left|\langle\psi_f|\tau\rangle\right|^2 \geq \frac{\|\Re(|\tau\rangle)\|_1^2}{\sqrt{2^n}} \geq \Omega(1)$$

Can we find a decent phase state that approximates the solution to the local Hamiltonian problem? (H, a, b)?

Yes, if $b - a = 1/\mathrm{poly}(n)$ and there exists a witness state $|\tau\rangle$ s.t.

$$\|\Re(|\tau\rangle)\|_1^2 \geq \Omega(\sqrt{2^n})$$

Creating a witness for (H, a, b)

- Assume wlog $0 \leq \|H\| \leq 1$.
- Let D be a random Clifford (or 2-design). Then whp
$$|\tau\rangle = (1 - H)^{O\left(\frac{n}{b-a}\right)} D|0^n\rangle$$
is an unnormalized state of energy $\leq a + (b - a)/2$.
- Problem is $|\tau\rangle$ may not have satisfy $\|\Re(|\tau\rangle)\|_1^2 \geq \Omega(\sqrt{2^n})$
- Whp $\|\Re(C|\tau\rangle)\|_1^2 \geq \Omega\left(\sqrt{2^n}\right)$ where C is a random Clifford
- **Thm 1**: $f(x) = \operatorname{sgn} \Re \langle x|C\ (1 - H)^{O\left(\frac{n}{b-a}\right)} D|0^n\rangle$ is in PP and whp
$$\left|\langle\psi_f|C|\tau\rangle\right|^2 \geq \frac{1}{1024}$$

Creating a witness for (H, a, b)

- **Thm 1**: $f(x) = \operatorname{sgn} \Re \langle x|C\ (1-H)^{O\left(\frac{n}{b-a}\right)} D|0^n\rangle$ is in PP and whp
$$\left|\langle \psi_f|C|\tau\rangle\right|^2 \geq \frac{1}{1024}$$
- Run phase estimation on $C^*|\psi_f\rangle$ which will with probability $\sim \frac{1}{1024}$ collapse to a state of energy $\leq a + (b-a)/2$.
- Can be run in parallel to amplify to $1 - 1/\exp(n)$ success pr.
- Still one query but on more qubits.

Can we do even better?

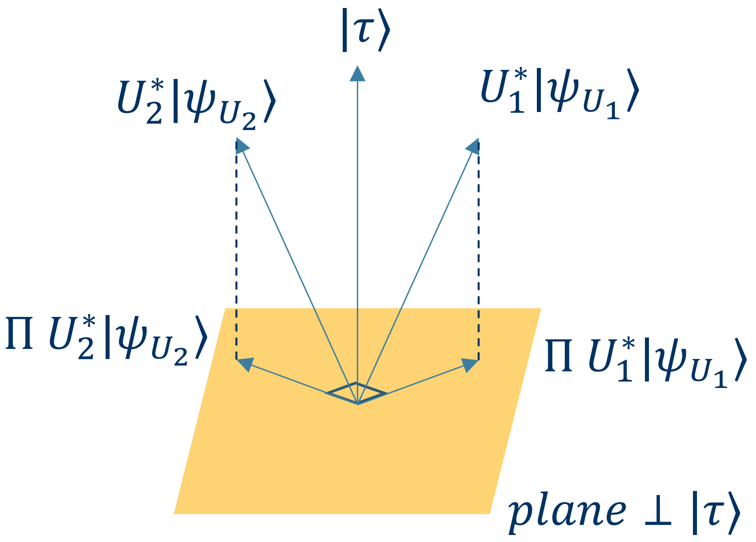
- Can we improve the complexity of the oracle query from PP to a smaller class (ideally QMA), perhaps at the cost of increasing the number of oracle queries?
- **Bound 1:** Given PGQMA = PP, a similar proof for PGQMA also yields a 1-query search-to-decision reduction for PGQMA
- **Bound 2**: There exists a 1-query search-to-decision reduction with pr 1 for UQCMA and pr $\Omega(1/n)$ for QCMA
- So, any proof would have to "thread the needle"
- **Theorem 2:** Modulo an oracle, QMA doesn't have search-to-decision

Rough sketch of oracle no-go result

- Inspiration is Aaronson-Kuperberg QCMA/QMA separator
- Oracle is a hidden-state oracle $\mathcal{O} = I - 2|\psi\rangle\langle\psi|$ or $\mathcal{O} = I$
- QMA problem is to decide which oracle it is
- Rough idea is that any witness to the problem must be $|\psi\rangle$
- And queries to $\mathcal{O}$ or any $\mathrm{QMA}^{\mathcal{O}}$ oracle don't reveal much about $|\psi\rangle$
- Hybrid argument cleans up details for complete lower bound

Improving state synthesis

- Say we want to synthesize a state $|\tau\rangle$
- We can pick a unitary U and create the best phase state estimate $|\psi_U\rangle$ for $U|\tau\rangle$. Then $U^*|\psi_U\rangle$ is a decent estimate for $|\tau\rangle$.



- And, two estimates are approximately orthogonal in the plane $\perp |\tau\rangle$
- If we apply SWAP test on two estimates, conditioned on passing, the remaining state points in the $|\tau\rangle$ direction more.

Improving state synthesis

- **Theorem 3:** There exists a 1-query algorithm with polynomial space and exponential time that synthesizes a state ρ such that $\langle\tau|\rho|\tau\rangle \geq 1 - 1/q(n)$ for any poly $q(n)$.
- Can we make the algorithm exponentially accurate? Yes, but we need another trick.
- The uniform distribution is an ok approximation for a Haar random state. Because Haar random states have a different profile: Porter-Thomas, which is constant distance away from uniform.

Exponentially accurate state synthesis

- Fix a universal state $|\theta\rangle$ such that whp over Haar random state $\sum_x \alpha_x |x\rangle$, there exists a permutation σ such that

$$\left\| |\theta\rangle - \sum_x |\alpha_x| \, |\sigma(x)\rangle \right\|$$

is exponentially small.
- Proof uses bounds from the theory of optimal transport
- Then only 2 queries are needed. One to specify σ and the phase angles and another to uncompute.

Open questions

- Can we improve our arguments for state synthesis using k-designs instead of Haar random unitaries?
- Can we argue PP hardness of any phase state with constant overlap with QMA witnesses (not the same as groundstates)?
- What is the power of $\mathrm{BQP}^{\mathrm{QMA}}$? It may not contain $\mathrm{SearchQMA}$ but does it contain any other non-trivial classes?
- What does all of this tell us about the unitary synthesis problem? Unitary synthesis is possible given state synthesis and post-selection.