QMA(k) – QMA with k unentangled provers

Main Reference: Harrow & Montanaro, arXiv: 1001.0017

Goal: $QMA^{SEP}(k) = QMA^{SEP}(2)$

Def^n A language $L \in QMA(k)_{s,c}$ if $\exists$ poly time quantum alg^m A s.t. for all inputs $x \in \{0,1\}^n$

- Completeness: if $x \in L$, $\exists$ k witnesses $|\psi_1\rangle, \ldots, |\psi_k\rangle$, each a state of poly(n) qubits, s.t. A accepts input $|x\rangle|\psi_1\rangle \ldots |\psi_k\rangle$ w. prob $\geq c$.
- Soundness: If $x \notin L$, A accepts w. prob $\leq s$ for all possible witnesses.

Assume $1 \leq k \leq poly(n)$. $QMA(k) = QMA(k)_{\frac{1}{3},\frac{2}{3}}$

$QMA_m(k)$ – using m qubits.

$QMA^{SEP}(k)$ – Only Separable measurements allowed

Classically could concatenate proofs: MA(k) = MA

Single Merlin could cheat in "QMA(k) = QMA" by entangling the k proofs. Need some way of preventing this.

Examples

Liu, Christandl, Verstraete quant-ph/0609125

"Pure state N-Representability" is in QMA(2) but not necessarily in QMA.

Given a 2-fermion density matrix ρ, decide whether N fermions, d modes, $d \leq poly(N)$.

YES: $\exists$ pure N-fermion state σ s.t. $tr_{3,\ldots,N}(\sigma) = \rho$.

NO: for all N-fermion states σ, $\|tr_{3,\ldots,N}(\sigma) - \rho\|_1 \geq \beta$

$\beta = \frac{1}{poly N}$

Without "pure", problem is QMA-complete

Focus on "pure": Arthur receives $\rho \otimes \sigma$ and calculates $\mathrm{tr}(\rho\sigma)$, which is close to 1 iff ρ is pure and $\rho \approx \sigma$.

Indeed if $\mathrm{tr}(\sigma^2) \leq 1-\varepsilon$, then $\forall \tau$

$\mathrm{tr}(\sigma\tau) \leq \sqrt{\mathrm{tr}(\sigma^2)\mathrm{tr}(\tau^2)} \leq (1-\varepsilon)^{\frac{1}{2}} \leq 1 - \varepsilon/2$.

So can test for purity if guaranteed to have product state. Only 1 merlin - Merlin can't defeat this test using entanglement.

Example:

Chailloux & Sattath, 1111.5217

"Separable Sparse Hamiltonian" is QMA(2)-complete

Sparse: only poly. many nonzero entries in each row & col

Like local Ham^n: energy $\leq a$ or $\geq b$

But also given partition of qubits: $\exists$ sep. state with energy $\leq a$ or all $\geq b$?

Try Local Ham^n proof: but entanglement in history states & superposition over time.

Use HM to convert into separable problem

But propagation terms C-SWAP is nonlocal but is sparse.

$\exists$ short quantum proofs for NP-complete problems

$\exists$ Protocol in QMA(2) that verifies 3-SAT with constant soundness gap using $O(\sqrt{n}\,\mathrm{polylog}(n))$ qubits. n = # clauses. n_1 variables, $n \geq n_1$.

2 Results:

- $QMA(2) = QMA(k)$
- Amplification of c & s

Theorem 9: If $c - s \geq \frac{1}{poly(n)}$, $k = poly(n)$, $p(n)$ poly,

$QMA(k)_{s,c} = QMA^{SEP}(2)_{\exp(-p(n)),\, 1-\exp(-p(n))}$.

Parallel repetition does not quite work due to entanglement swapping: $M_1, \ldots, M_k$ each send & unentangled states but Arthur's measurement on first state may result in remaining states being entangled.

e.g. 2 Merlins each sending 2 qubits. (each proof is 1 qubit.)
Each cheats and sends $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
Arthur measures first qubit in Bell basis.
Second qubits are now entangled.

Key Ingredient:
Protocol 1: Product Test

- Receive 2 copies of $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$.
  Call them $|\psi_1\rangle$ & $|\psi_2\rangle$.
- Perform SWAP Test on each of the n pairs of corresponding subsystems.
- If all tests return "same", accept. Otherwise reject

Theorem 1: Given $|\psi\rangle \in \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$, let

$1 - \varepsilon = \max\{ |\langle\psi| \phi_1 \phi_2 \cdots \phi_n\rangle|^2 : |\phi_i\rangle \in \mathbb{C}^{d_i} \}$

$P_{test}(|\psi\rangle\langle\psi|)$ = Prob Product test accepts $|\psi\rangle$

Then $P_{test}(|\psi\rangle\langle\psi|) = 1 - \Theta(\varepsilon)$.

Protocol 2: $QMA(k) \to QMA(2)$

1. Each of the 2 Merlin sends $|\psi\rangle = |\psi_1\rangle \ldots |\psi_k\rangle$.
2. With Prob $\frac{1}{2}$, Arthur
   (a) Runs the product test and accepts iff the test outputs products
   or (b) randomly chooses state from M_1 or M_2 and applies the $QMA(k)$ algorithm to it.

Lemma 6: For any m, k, $0 \le s < c \le 1$
$QMA_m(k) \subseteq QMA^{SEP}_{km}(2)_{s',c'}$
with $c' = \frac{1+c}{2}$, $s' = 1 - \frac{(1-s)^2}{100}$

Proof:
Completeness: k Merlins can achieve success prob c. 2 copies of this optimal state will succeed w. prob $\geq \frac{1+c}{2} \geq c$.

Soundness:
Product test $\Rightarrow$ close to product
Continuity argument $\Rightarrow$ success prob not much larger than soundness of original protocol.

Arthur receives $|\phi_1\rangle, |\phi_2\rangle$ s.t. maximal overlap w. product state is $1-\varepsilon_1$, $1-\varepsilon_2$ respectively.
Assume product test would accept $|\phi_i\rangle^{\otimes 2}$ w. prob $1-\delta_i$. $\delta = \frac{1}{2}(\delta_1 + \delta_2)$, $\varepsilon = \frac{1}{2}(\varepsilon_1 + \varepsilon_2)$.
$1-\delta$ = prob. $|\phi_1\rangle|\phi_2\rangle$ passes product test.

Then

$$1-\delta = \mathrm{tr}\left(|\phi_1\rangle\otimes|\phi_2\rangle\left(\frac{I+F}{2}\right)^{\otimes k}\right)$$

$F|ij\rangle = |ji\rangle$ flip.

$$= \frac{1}{2^k}\sum_{S\subseteq[k]}{}' \mathrm{tr}\left(|\phi_1\rangle\otimes|\phi_2\rangle F_S\right)$$

F_S = flip on subspaces indexed by elements in S.

$\phi_i^2 = |\phi_i\rangle\langle\phi_i|$

$$= \frac{1}{2^k}\sum_{S\subseteq[k]}{}' \mathrm{tr}\left((\phi_1)_S\,(\phi_2)_S\right)$$

$$\leq \frac{1}{2^k}\sum_{S\subseteq[k]}{}' \sqrt{\mathrm{tr}(\phi_1)_S^2}\,\sqrt{\mathrm{tr}(\phi_2)_S^2}$$

$$\leq \frac{1}{2^k}\sum_{S\subseteq[k]}{}' \frac{\mathrm{tr}(\phi_1)_S^2 + \mathrm{tr}(\phi_2)_S^2}{2}$$

$$= 1 - \tfrac{1}{2}(\delta_1+\delta_2)$$

Theorem 1, $\delta \geq \frac{11}{512}\varepsilon$. $\quad \delta_i \longleftrightarrow \varepsilon_i$, $\delta \longleftrightarrow \varepsilon$.

Lemma 22: If $|\psi\rangle, |\phi\rangle$ are pure states, and $|\langle\psi|\phi\rangle|^2 = 1-\varepsilon$, $0\leq P\leq I$

Then $|\langle\psi|P|\psi\rangle - \langle\phi|P|\phi\rangle| \leq \sqrt{\varepsilon}$.

Proof: $\frac{1}{2}\left\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\right\|_1 = \sqrt{\varepsilon}$

$\Rightarrow \left|\mathrm{tr}\left(P(|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|)\right)\right| \leq \sqrt{\varepsilon}$.

So if Arthur is in case (b), and makes a measurement P, prob. accepting

$$\leq s + \frac{\sqrt{\varepsilon_1}+\sqrt{\varepsilon_2}}{2} \leq s + \sqrt{\varepsilon}$$

Altogether prob accepting is

$$s' \leq \max_{\varepsilon \leq \frac{512}{11}\delta} \frac{1-\delta+\min(1, s+\sqrt{\varepsilon})}{2}$$

Worst case when $\sqrt{\varepsilon} = 1-\delta = \sqrt{\frac{512}{11}\delta}$. $\rightarrow$ Result

Accept Measurement is Separable:

M_1 sends $A_1 A_2 \cdots A_k$

M_2 " $B_1 B_2 \cdots B_k$

(a) "Accept" = $\otimes$ projection onto symmetric subspaces of $A_1B_1, \ldots, A_kB_k$

But each of these subspaces is spanned by $\{|\psi\rangle|\psi\rangle\}$ and thus these projections are separable.

(b) Entirely on $A_1, \ldots A_k$ or entirely on $B_1 \ldots B_k$

Probabilistic mixture of separables is separable. ▨

Lemma 7: For any $\ell \geq 1$,

$QMA^{SEP}_m(k)_{s,c} \subseteq QMA^{SEP}_{\ell m}(k)_{s^\ell, c^\ell}$

Proof: Original protocol, Arthur performs measurement M on k states each of m qubits.

YES: $\exists$ product state, w. success prob $\geq s$

NO: $\forall$ product states, " " $\leq s$.

Modified protocol:

Each of k prover submits ℓm qubits.

Arthur measures w. $M^{\otimes \ell}$.

YES: ℓ copies of original input.

NO:

Imagine sequentially measuring w. $\{M, I-M\}$ accepting only if output is M each time.

If applied to a separable state each time, each will have prob $\leq s \rightarrow s^\ell$.

But as M is separable, it outcome

M occurs, no entanglement is created across k provers.
(and if $I-M$, reject, so does not matter) ▨

Aaronson et al

Lemma 8: For any $\ell \geq 1$,

$$QMAm(k)_{s,c} \subseteq QMA_{em}(k)_{1-\frac{c-s}{3},\, 1-\exp(-\ell(c-s)^2/2)}$$

Proof: Repeat basic protocol ℓ times and accept if there are $\geq \frac{c+s}{2}\ell$ "accepts".

YES: ℓ copies of same proof, each accepted w. prob $\geq c$. Chernoff bound.

$$1-\exp(-\ell(c-s)^2/2).$$

NO: Each of the ℓ copies has prob $\leq s$ of acceptance. No longer independent perhaps, but Markov's inequality $\Rightarrow$

$$\text{prob}(\geq \tfrac{c+s}{2}\ell \text{ accepts}) \leq \frac{2s}{c+s} = \frac{1}{1+(c-s)/2} \leq 1 - \frac{c-s}{3}$$

Using $\frac{1}{1+x/2} \leq 1 - x/3$ for $0 \leq x \leq 1$. ▨

Theorem 9: (1) If $s \leq 1 - \frac{1}{poly(n)}$, $k = poly(n)$, $p(n)$ poly

Then $QMA(k)_{s,1} = QMA^{SEP}(2)_{\exp(-p(n)),\, b}$

2. $c - s \geq \frac{1}{poly(n)}$, $c < 1$, ...

$$QMA(k)_{s,c} = QMA^{SEP}(2)_{\exp(-p(n)),\, 1-\exp(-p(n))}$$