QMA(2) workshop— Tutorial 1

Bill Fefferman
(QuICS)

Agenda

I. Basics
II. Known results
III. Open questions/Next tutorial overview

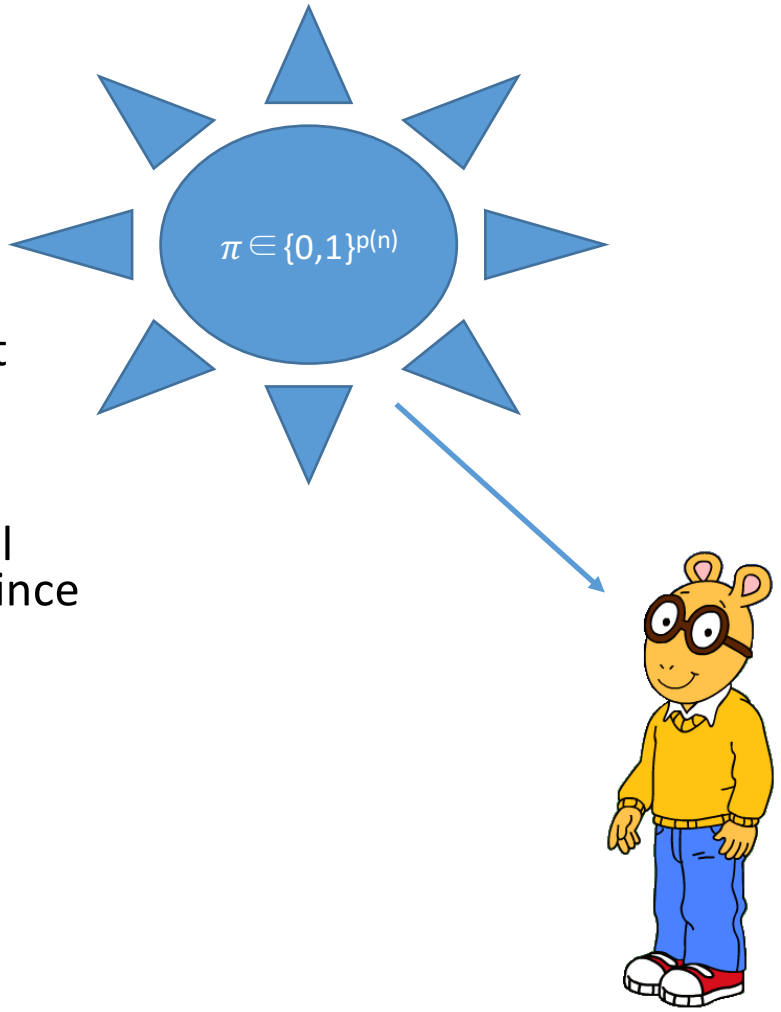
I. Basics

I.1 Classical Complexity Theory

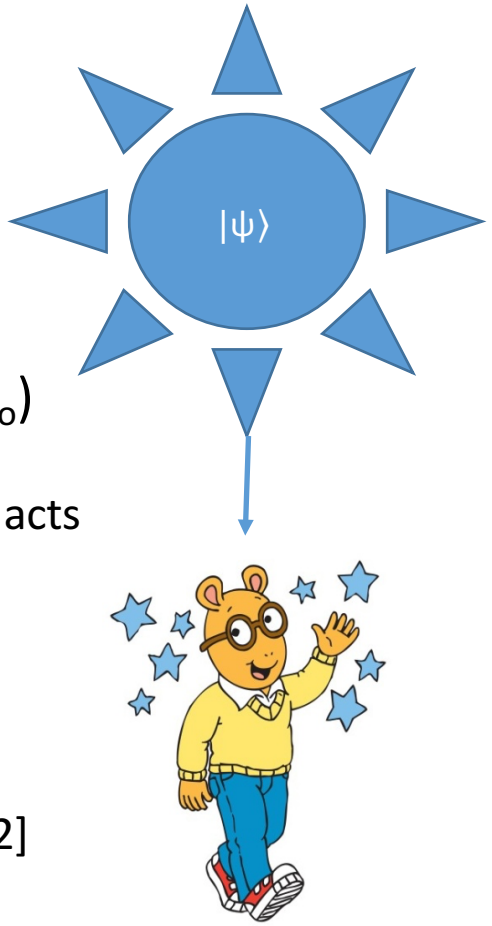
- **P**
  - Class of problems efficiently solved on classical computer
- **NP**
  - Class of problems with efficiently verifiable solutions
  - Characterized by **3SAT**
    - Input: $\Psi:\{0,1\}^n \rightarrow \{0,1\}$
      - n-variable 3-CNF formula
        - E.g., $(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_6) \wedge \ldots$
    - Problem: $\exists\, x_1, x_2, \ldots, x_n$ so that $\Psi(x)=1$?
  - Could use a box solving **3SAT** to solve any problem in **NP**

I.2 *Merlin-Arthur*

- "Randomized generalization" of **NP**
- Can think of a game between all-knowing but potentially dishonest Merlin trying to prove statement to efficient randomized classical computer (Arthur)
- If statement is *true*, there exists a polynomial length classical bitstring or "witness" to convince Arthur to accept *with high probability* (*Completeness*)
- If statement is *false*, then every "witness" is rejected by Arthur *with high probability* (*Soundness*)
- Under commonly believed derandomization hypothesis **MA**=**NP**



I.3 *Quantum Merlin-Arthur*



- **QMA**: Same setup, now Arthur is **BQP** machine,
  witness is polynomial qubit quantum state
- *Formally*: **QMA**$_m$ is the class of promise problems L=(L_{yes},L_{no}) so that:
  - There exists a uniform verifier $\{V_x\}_{x\in\{0,1\}^n}$ of polynomial size that acts on O(m(|x|)+k(|x|)) qubits (for k∈poly(n)):

$$x \in L_{yes} \Rightarrow \exists|\psi\rangle \ \left(\langle\psi| \otimes \langle 0^k|\right) V_x^\dagger |1\rangle\langle 1|_{out} V_x \left(|\psi\rangle \otimes |0^k\rangle\right) \geq 2/3$$
$$x \in L_{no} \Rightarrow \forall|\psi\rangle \ \left(\langle\psi| \otimes \langle 0^k|\right) V_x^\dagger |1\rangle\langle 1|_{out} V_x \left(|\psi\rangle \otimes |0^k\rangle\right) \leq 1/3$$

- "Quantum analogue" of **NP**
- *k-Local Hamiltonian* problem is **QMA**-complete (when k≥2) [Kitaev '02]
  - Input: $H = \sum_{i=1}^{M} H_i$, each term H_i is k-local
  - Promise, for (a,b) so that b-a≥1/poly(n), either:
    - $\exists\,|\psi\rangle\ so\ that\ \langle\psi|\mathrm{H}|\psi\rangle \leq$ a *OR*
    - $\forall\,|\psi\rangle\ we\ have\ \langle\psi|\mathrm{H}|\psi\rangle \geq$ b

I.4 Entangled quantum states

- Let A and B be two finite dimensional complex vector spaces
- A bipartite density matrix, or state, is a positive semidefinite matrix ρ_{AB} on $A \otimes B$ that has unit trace
- ρ_{AB} is called *separable* if it can be written as $\rho_{AB} = \sum_k p_k \rho_{A,k} \otimes \rho_{B,k}$
  - For local states $\{\rho_{A,k}\}$ and $\{\rho_{B,k}\}$ and probabilities p_k
- States that are not *separable* are *entangled*

I.5 QMA(2): The power of separable witness

- Our question: Is there an advantage to Merlin sending unentangled states?
  - **QMA**(2):
    - *Completeness*: There exist state $|\psi_1\rangle \otimes |\psi_2\rangle$ that convinces Arthur to accept with high probability
    - *Soundness*: All states $|\psi_1\rangle \otimes |\psi_2\rangle$ are rejected by Arthur with high probability
  - **QMA**(k): Same class with *k* witnesses
- Trivial bounds: **QMA** $\subseteq$ **QMA**(2) $\subseteq$ **NEXP**
- Why isn't **QMA**(2) *obviously* contained in **QMA**?
  - Merlin can cheat by entangling, and checking separability is hard
    - E.g., "**Weak-membership**(ε)" is **NP**-hard [e.g., Gharibian'09]
      - Given ρ_{AB} is it separable or $|\rho_{AB}\text{-Sep}|>\varepsilon$?
      - Where $\varepsilon=1/\text{poly}(|A|,|B|)$ relative to the trace norm
- Error amplification is non-trivial
    - Repetition doesn't work (Measurements on one set of copies can create entanglement between witnesses)

I.6 Why should *you* care about QMA(2)?

- There are many multi-prover quantum complexity classes, why should we care about this one?

1. Connections to separability testing (i.e., given a quantum state is it separable or far from separable?)
2. Connections to entanglement measures and "quantum de Finetti theorems"
3. Close connections to hardness of approximation and classical complexity theory: "Unique Games Conjecture" and the "Exponential Time Hypothesis"

I.7 Classes of bipartite measurement operators e.g., HM'12

- There's an interesting line of work attempting to understand **QMA**(2) with restricted verification protocols
- We say a **POVM** (M,I-M) is in:
- BELL : "systems are measured locally with no conditioning" $M = \sum_{(i,j)\in S} \alpha_i \otimes \beta_j$
  - Where $\sum_i \alpha_i = I$ and $\sum_i \beta_i = I$
  - S is set of pairs of outcomes (indices)
  - i.e., systems are measured locally get outcome (i,j) and accept iff (i,j)$\in$S
- 1LOCC: "choose measurement on system B conditioned on outcome of measurement on system A" $M = \sum_i \alpha_i \otimes M_i$
  - Where $\sum_i \alpha_i = I$ and $0 \le M_i \le I$ for each M_i
  - Can be generalized to LOCC by allowing for finite number of rounds of alternating measurements on the two subsystems
- SEP is the class of measurements M so that $M = \sum_i \alpha_i \otimes \beta_i$
  - For positive semidefinite matrices $\{\alpha_i\}$ and $\{\beta_i\}$
- Notice that BELL$\subseteq$ LOCC1$\subseteq$ LOCC$\subseteq$ SEP$\subseteq$ ALL

II. Results on QMA(2)

II.1. SAT protocol: Aaronson, Beigi, Drucker, F., Shor '09

- Conjecture 1: **3SAT$_n$** cannot be solved in *classical* poly(n) time
  - Equivalent to **NP⊄P**
- Conjecture 2: **3SAT$_n$** cannot be solved in *classical* $2^{o(n)}$ time
  - "Exponential-time Hypothesis" [Impagliazzo & Paturi '99]
  - Seems reasonable even quantumly – "*Quantum* ETH"
- Our result: $\mathbf{3SAT_n} \in \mathbf{QMA}_{\log n}(\tilde{\mathcal{O}}(\sqrt{n}))$
  - i.e., sqrt(n) witnesses, each on log(n) qubits (*here n is number of clauses)
  - Notice total number of witness qubits is o(n)
  - Same result classically would show Exponential-time Hypothesis to be false
- Proof idea:
  - Suppose $x_1,x_2,\ldots,x_n \in \{0,1\}^n$ is Merlin's claimed satisfying assignment
  - Ask all Merlins to send the same state: $\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(-1)^{x_i}|i\rangle$
  - Need many Merlins to check that he sent this state!

II.1 (part ii). Related QMA(2) protocols

- Related protocols:
  - [Blier & Tapp '09] $\mathbf{NP} \subseteq \mathbf{QMA}_{\log n}(2, 1, 1 - \frac{1}{poly(n)})$
    - Via protocol for **3Coloring**
    - If soundness was constant then **NEXP**$\subseteq$**QMA**(2)
  - [Chen & Drucker '10] $\mathbf{3SAT_n} \in \mathbf{QMA}^{\mathrm{BELL}}_{\log n}(\tilde{O}(\sqrt{n}))$
    - Verifier uses local measurements
    - Matches parameters of [ABDFS'09]
      - Perfect completeness and constant soundness

II.2. "Product test": Harrow & Montanaro '12

- For all k≤poly(n) **QMA**(k)=**QMA**(2)
  - Uses the "product test"
  - Ask both Merlins to send $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes \ldots \otimes |\psi_k\rangle$
  - Pr ½: Arthur "swap tests" on each of the k pairs of corresponding subsystems and accepts iff they all accept
    - Swap test on states ρ and σ accepts with probability 1/2+1/2 Tr[ρσ]
  - Pr ½: Arthur runs verification protocol on one of the states
- *Main result*:
  - Suppose we are given two copies of k-partite state $|\psi\rangle$
  - Let $1-\epsilon = \max_{|\phi\rangle \in Sep(k)} \{|\langle\psi|\phi\rangle|^2\}$
  - Then Product test accepts with probability $1-\Theta(\epsilon)$
- In fact, **QMA**(k)=**QMA**^{Sep}(2)
  - Because the "accept" measurement of product test is separable operator

II.2 (part ii). More consequences of [HM'12]

1. Improves the **SAT** protocol from before [ABDFS'09]
   1. Result as stated: $\mathbf{SAT_n} \in \mathbf{QMA}_{\log n}(\tilde{\mathcal{O}}(\sqrt{n}))$
   2. Result together with [HM'12]: $\mathbf{SAT_n} \in \mathbf{QMA}_{\tilde{\mathcal{O}}(\sqrt{n})}(2)$
   3. Don't know how to extend this to Chen & Drucker result
2. Hardness consequences for "**ε-Best Separable State**" problem
   - *Input*: Hermitian matrix M on $A \otimes B$
   - *Output*: Estimate of $\mathbf{h_{Sep}}(M)=\max_{\sigma \in Sep} Tr[M\sigma]$ to within additive error ε
   - "Equivalent" in hardness to Weak Membership problem
     - So this problem is **NP**-hard for ε=1/poly(d)
   - Notice that this problem is at least as hard as deciding a language in **QMA**(2)
     - Therefore, $\mathbf{SAT_n}$ can be cast as a **BSS** problem with $|A|=|B| \approx 2^{O(\sqrt{n})}$
     - Gives subexponential bounds on the complexity of ε-Best Separable State for constant ε
     - Suppose there's an algorithm runs in time $\exp(O(\log^{1-\gamma}|A|\log^{1-\nu}|B|)$ then ETH is false!
   - **ε-Best Separable State** turns out to also be polynomial-time equivalent to many other problems
     - Connections to Unique Games conjecture via "2-to-4 norm problem" (see [HM'12] for details)
3. Is **QMA**(2)⊆**QMA**?
   - $\mathbf{QMA_m}(1) \subseteq \mathbf{BQTIME}[O(2^m)]$ [Marriott & Watrous '04]
   - So, if $\mathbf{QMA_m}(2)=\mathbf{QMA}_{m^{2-\nu}}$ the Quantum ETH is false
4. $\mathbf{QMA}^{Sep}(2)$ characterization allows us to error amplify using repetition!

II.3. QMA(2) with 1LOCC measurements [BCY'11]

- "Quantum de Finetti" Theorem
  - *Definition*: We say a bipartite state ρ_{AB} is *k-extendible* if:
    - There exists a (k+1)-partite $\rho_{AB_1B_2\ldots B_k}$ so that $\rho_{AB} = \rho_{AB_1} = \rho_{AB_2} = \ldots = \rho_{AB_k}$
  - *Separable* states are k-extendible for all k>0 [e.g., DPS'08]
  - [Christandl et. al '07] shows that k-extendible states are close to separable in a well-defined sense:
    $$||\rho_{AB} - Sep||_1 \leq \frac{4|B|^2}{k}$$
  - [BCY'11] shows much tighter relation for 1LOCC norm:
    $$||\rho_{AB} - Sep||_{1\text{LOCC}} \leq \sqrt{\frac{\log|A|}{k}}$$
  - As a consequence, $\mathbf{QMA}_m^{1\text{LOCC}}(2) = \mathbf{QMA}_{m^2}(1)$
    - *Proof idea*: In QMA(1) protocol, Arthur asks Merlin to send k-extension of his bipartite witness
    - Use de Finetti theorem for 1LOCC to bound soundness probability (i.e., the advantage Merlin gets from entangling his states in case the answer is 'No')
- There's an interesting line of work trying to improve this result in various ways e.g., [Brandao & Harrow '11], [Lancien & Winter'16]

II.4. Complete problem for **QMA**(2) [Chailloux & Sattath '12]

- *Recall*: "k-local Hamiltonian problem" is **QMA**-complete
- "Separable sparse Hamiltonian problem"
  - *Definition*: An operator over n qubits is *row-sparse* if:
    - Each row in A has at most poly(n) non-zero entries
    - There's classical algorithm that takes a row index and outputs the non-zero entries this row
  - *Input*: Row-sparse Hamiltonian, H, on n qubits
  - *Promise*: for (a,b) so that b-a≥1/poly(n), either:
    - $\exists\, |\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B \; so\ that\ \langle\psi|H|\psi\rangle \leq a$ *OR*
    - $\forall\, |\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B \; we\ have\ \langle\psi|H|\psi\rangle \geq b$
- Proof uses "clock" construction of Kitaev and "Product test" of Harrow-Montanarc
- In fact, same paper shows that Separable *local* Hamiltonian is **QMA**-complete
- Starting point for recent attempt at proving **QMA**(2) upper bound [Schwarz'15]

III. Open questions/Preview of things to come

III. Open Questions

- Can we put a nontrivial upper bound on **QMA**(2)?
- Can Chen & Drucker's 3SAT protocol with BELL measurements be improved to use only 2 witnesses?
- Can the 1LOCC de Finetti theorem be extended to SEP? measurements? This would imply **QMA**(2)$\subseteq$ **QMA**(1)
- **QMA**(1)=**QMA**^{1LOCC}(2) vs **QMA**^{SEP}(2)=**QMA**(k)
- Other **QMA**(2)-complete problems?

III. Next time!

- Classical complexity of the ε-Best Separable State problem

1. SDP hierarchies and its relation to BSS
   - Give algorithms for (special cases) of BSS
     - "Sum-of-Squares"
2. ε-nets