Quantum vs Classical Proofs and In-place Oracles

Bill Fefferman (QuICS, UMD/NIST)

Joint with Shelby Kimmel (QuICS, UMD/NIST)

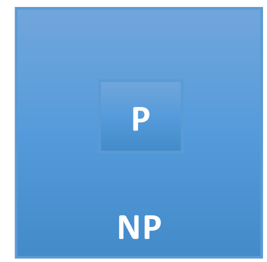
Outline

- Basics
- “Quantum oracles”
- **QMA**/**QCMA** oracle separation

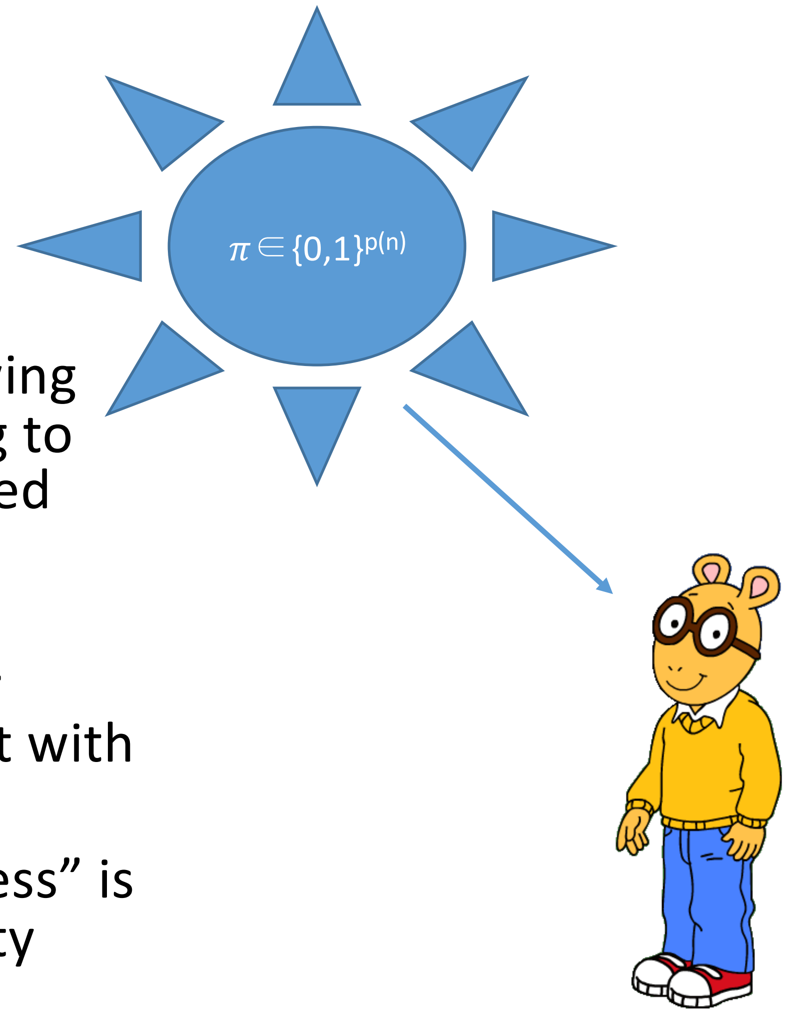
1. Basics

Classical Complexity Theory

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

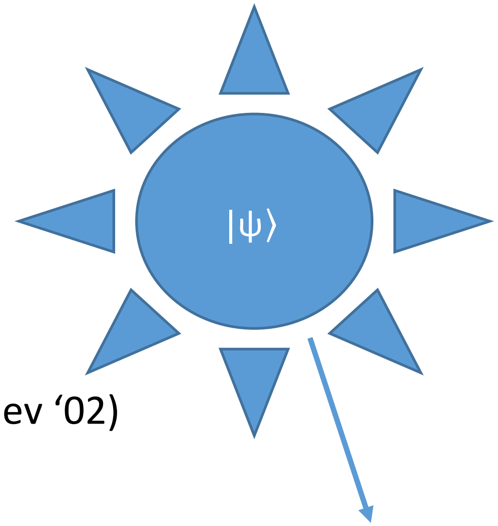


Merlin-Arthur



- "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
- If statement is *false*, then every "witness" is rejected by Arthur with high probability

Quantum Merlin-Arthur



- **QMA**: Same setup, now Arthur is **BQP** machine,
  witness is polynomial qubit quantum state
- *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* $\langle\psi|H|\psi\rangle \leq$ a
    - $\forall|\psi\rangle:\ \langle\psi|H|\psi\rangle \geq$ b
- Our question: Is there an advantage to quantum witness?
  - **QCMA**: The witness is classical basis state
  - **QCMA** $\subseteq$ **QMA** (trivial)
  - Is **QMA**$\subseteq$**QCMA**? (Aharonov & Naveh '04)
    - AN'04 conjecture the answer is *yes* (because it's feasible that for every k-local Hamiltonian there exists some efficient quantum circuit that prepares the ground state)
    - But we still have few formal results about this question…

2. “Quantum oracles”

Variants of quantum "oracle"

- "Standard"
  - Given $f:\{0,1\}^n \rightarrow \{0,1\}^m$
  - $U_f: |x>|y> \rightarrow |x>|y \oplus f(x)>$
  - Notice $U_f = U_f^{-1} \neq U_{f^{-1}}$
- "In-place" (Kashefi et. al. '01, de Beaudrap et. al.'01, Aaronson '02…)
  - Given permutation $\sigma:[N] \rightarrow [N]$
  - $P_\sigma: |i> \rightarrow |\sigma(i)>$
  - Notice $P_\sigma \neq P_{\sigma^{-1}} = P_\sigma^{-1}$
- "Quantum Oracle" (e.g., Aaronson & Kuperberg '07)
  - Quantum algorithm can apply black-box unitary $\{U_n\}$
- Finding oracle separations between complexity classes is a often far easier problem than the unrelativized separation, but what do they actually tell us?
  - Tell us about proof techniques that don't suffice
  - *My motivation*: If we don't know how to find a relativized separation we are incredibly ignorant about the underlying complexity classes.

“Standard” vs “in-place” oracles

- Are there tasks that we can accomplish with dramatically fewer queries in either model?
- In-place > standard
  - Consider σ:[N^2]→[N^2], want to prepare $\frac{1}{\sqrt{N}}\sum_{i\in[N]}$ |σ(i)>
  - Requires 1 query to “in-place” σ
    - Prepare $\frac{1}{\sqrt{N}}\sum_{i\in[N]}$ |i>
    - Query “in-place” σ
  - Requires Ω($\sqrt{N^2}$) =Ω(N) queries with “standard” σ (Ambainis et. al., ‘10)
    - Related to “index erasure” problem
      - i.e., can prepare $\frac{1}{\sqrt{N}}\sum_{i\in[N]}$ |i>|σ(i)> with one standard query
      - To “erase index” requires Ω(N) queries
- Standard > In-place
  - Suppose $S \subseteq [N^2]$, given $\frac{1}{\sqrt{|S|}}\sum_{i\in S}$ |i>|σ(i)>, want to prepare $\frac{1}{\sqrt{|S|}}\sum_{i\in S}$ |i>|0>
  - Can do this with 1 query to standard oracle for σ
  - Seems harder for an In-place σ…
  - How about inverting permutation?
    - i.e., is $\sigma^{-1}(1)$ odd or even?
    - Requires $\sqrt{N^2}$=N standard queries (Ambainis ’00)
    - We show it requires N in-place queries, conjecture it requires N^2 (no Grover for in-place oracles!)

3. QMA/QCMA oracle separations

Past work: Aaronson & Kuperberg '07

- Result $\exists \{U_n\}$ **QMA**$^{\{U_n\}} \not\subset$ **QCMA**$^{\{U_n\}}$
- Choose an n-qubit state $|\psi\rangle$ uniformly at random
- Define n+1 qubit unitary
  - U_ψ: $\begin{cases} |\psi\rangle|b\rangle \rightarrow |\psi\rangle|b\oplus 1\rangle \\ |\varphi\rangle|b\rangle \rightarrow |\varphi\rangle|b\rangle \ if \ \langle\psi|\varphi\rangle = 0 \end{cases}$
- *Problem*: "Identity checking": Given quantum oracle access to unitary U, promised either $U=U_\psi$ or U=Id. Which is the case?
- Identity checking is in **QMA**$^{\{U_n\}}$
  - Quantum witness is the state $|\psi\rangle$
- Not in **QCMA**$^{\{U_n\}}$
  - Proof by "Geometrical" lemma
    - *Intuition*: Polynomial classical bits are not enough to describe $|\psi\rangle$

What (else) are quantum proofs good for?

- First attempt to separate **QMA** from **QCMA** relative to standard oracle (*that doesn't work*)
  - Consider the following problem (and let $N=2^n$):
    - Given standard oracle access to $f:\{0,1\}^n \rightarrow \{0,1\}$ and promised either:
      - "Yes case": f has exactly $\sqrt{N}$ inputs that map to 1
      - "No case": f has at most $0.9\sqrt{N}$ inputs that map to 1
      - Which is the case?
    - First off: problem shouldn't be in **QCMA**
      - Intuition is clear: subset of inputs that map to one is unstructured and exponential in size
      - This can be formalized using e.g., quantum polynomial method
    - But is it in **QMA**?
      - Attempt: Ask Merlin to give you state uniformly supported on a subset $S \subseteq \{0,1\}^n$ of size exactly $\sqrt{N}$
        - i.e., honest Merlin sends $\frac{1}{\sqrt[4]{N}}\sum_{x\in S}|\mathrm{x}\rangle$
        - Now Arthur queries f in an output register:
          - $\frac{1}{\sqrt[4]{N}}\sum_{x\in S}|\mathrm{x}\rangle|0\rangle \rightarrow \frac{1}{\sqrt[4]{N}}\sum_{x\in S}|\mathrm{x}\rangle|\mathrm{f(x)}\rangle$
        - Measures output register and accepts iff he obtains 1
      - Notice if we could only be *certain* that Merlin sent us state uniformly supported on *exactly* $\sqrt{N}$ inputs, we'd be done
        - Note that in that "No case" the probability we accept is at most 0.9
      - But verifying that Merlin really sent this state seems extremely hard…

Our result: In-place oracle separation

- $\exists \{P_\sigma\}$ **QMA**$^{\{P_\sigma\}} \not\subset$ **QCMA**$^{\{P_\sigma\}}$
- Intuition:
  - σ:[N^2]→[N^2] , N=2^n
  - Inverting σ has exponential query complexity in standard oracle model
  - Suppose we could find a decision problem in which to decide "yes" from "no" requires preparing $\frac{1}{\sqrt{N}}\sum_{i\in[N]} |\sigma^{-1}(\mathrm{i})\rangle$
    - This problem would be in **QMA**$^{\{P_\sigma\}}$
      - Merlin sends $\frac{1}{\sqrt{N}}\sum_{i\in[N]} |\sigma^{-1}(\mathrm{i})\rangle$
      - Protocol is sound! Merlin can't cheat
        - Arthur applies P_σ and checks that the resulting state is $\frac{1}{\sqrt{N}}\sum_{i\in[N]} |\mathrm{i}\rangle$
    - This problem should not be in **QCMA**$^{\{P_\sigma\}}$
      - Preparing this state seems similar to permutation inversion
      - The polynomial length classical witness shouldn't help much…

Our (In-place) oracle problem

- *Definitions*: with respect to σ:[N^2]→[N^2]
  - Define S(σ)={j: $\sigma(\mathrm{j}) \in [N]$}
  - Call σ "Even" if S(σ) has 2/3 even elements (and also say S(σ) is "Even Preimage")
  - Call σ "Odd" if S(σ) has 2/3 odd elements (and also say S(σ) is "Odd Preimage")
- "*Preimage checking*": Given in-place oracle access to P_σ
  - "Yes case": σ is "Even"
  - "No case": σ is "Odd"
- *Preimage Checking* is in **QMA**$^{P_\sigma}$
  - Honest Merlin sends $\frac{1}{\sqrt{N}}\sum_{i\in[N]} |\sigma^{-1}(\mathrm{i})\rangle$
  - With probability ½ Arthur measures Merlin's state, accepts if even
  - With probability ½ Arthur runs in-place oracle on Merlin's state
    - Note that if Merlin is honest Arthur is left with $\frac{1}{\sqrt{N}}\sum_{i\in[N]} |\mathrm{i}\rangle$
    - Arthur can check this!

	"Yes"	"No"
$\sigma^{-1}(1)$	8	9
$\sigma^{-1}(2)$	2	2
$\sigma^{-1}(3)$	1	1
$\sigma^{-1}(4)$	3	3
$\sigma^{-1}(5)$	6	6
$\sigma^{-1}(6)$	7	7
$\sigma^{-1}(7)$	9	8
$\sigma^{-1}(8)$	5	5
$\sigma^{-1}(9)$	4	4

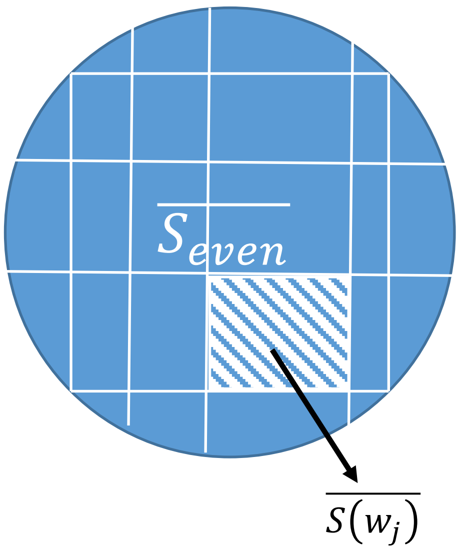
(example with N=3)

QCMA$^{\{P_\sigma\}}$ lower bound: Proof overview

- *(Rough) Goal*: Find infinite set of permutations $\{P_{\sigma,n}\}_{n\geq 1}$ and unary language L$\in$**QMA**$^{\{P_{\sigma,n}\}}$ so that for any **QCMA** machine M, $\exists$ n $M^{P_{\sigma,n}}(1^n) \neq L(1^n)$
- Fix an enumeration of all **QCMA** machines $M_0, M_1, M_2, \ldots$
- Will find, for each M_i some "Even" σ that cannot be distinguished by M from an "Odd" σ'
- This suffices to obtain our goal

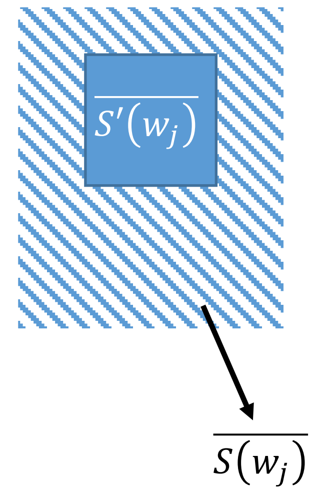
QCMA$^{\{P_\sigma\}}$ lower bound: Proof details (1)

- Step 1/3: "Witness conditioning"
  - Enumerate all quantum verifiers $M_0, M_1, M_2, \ldots$
  - For each fixed machine M_i:
    - There's a mapping that takes each "Even" preimage S to the best polynomial length witness for that preimage
      - i.e., the witness that convinces M_i to accept a permutation whose preimage is S with highest probability
  - Define $\overline{S_{even}} = \left\{ S \subset [N^2] \,\middle|\, |S| = N, |S \cap \mathbb{Z}_{even}| = \frac{2}{3}N \right\}$
  - Define $\overline{S(w)} \subseteq \overline{S_{even}}$ to be the set of even preimages in which w is the witness that leads M_i to accept with highest probability
    - Note that the sets $\{\overline{S(w_0)}, \overline{S(w_1)}, \ldots, \overline{S(w_{2^{p(n)}})}\}$ partition $\overline{S_{even}}$
    - Thus there must exist a w_j so that:
      - $|\overline{S(w_j)}| \geq |\overline{S_{even}}|/2^{p(n)}$
      - We will restrict ourselves to choosing an Even permutation with preimage in $\overline{S(w_j)}$
        - This effectively "hardwires" this w_j into M_i (since each even permutation now corresponds to the same witness)
        - Reduced the problem to a in-place oracle query problem
    - Will prove there exists an even σ such that $S(\sigma) \in \overline{S(w_j)}$ and still M_i requires exponential queries to decide if given in-place oracle access to σ or some "Odd" σ'



QCMA$^{\{P_\sigma\}}$ lower bound: Proof details (2)

- Step 2/3: "Fixing lemma":
  - *Definition*: $\bar{S} \subseteq \overline{S_{even}}$ is δ-distributed if:
    - There exists a set $S_{fixed} \subseteq [N^2]$ so that:
      1. S_{fixed} is a subset of every $S \in \bar{S}$
      2. $|S_{fixed} \cap \mathbb{Z}_{even}| \leq \frac{1}{3}N$ and $|S_{fixed} \cap \mathbb{Z}_{odd}| \leq \frac{1}{3}N$
      3. For every element $i \in [N^2]/S_{fixed}$, *i appears in at most* N^{δ} *fraction of* $S \in \bar{S}$
  - Goal: Output a set $S'(w_j) \subseteq \overline{S(w_j)}$ that is β-distributed (0≤β≤1)
    - Procedure works by starting with $\overline{S(w_j)}$
    - Until condition 3 above is satisfied:
      a) Take the i' that is in more than N^{δ} fraction of sets and add it to S_{fixed}
      b) Remove all sets that don't contain i'
      - Repeat steps a & b until condition 3 is satisfied
    - Note: counting argument shows that $\overline{S'(w_j)}$ satisfies property 2.



QCMA$^{\{P_\sigma\}}$ lower bound: Proof details (3)

- Step 3/3: "Query lower bound theorem for permutations whose preimage form a fixed subset system"
- *Theorem*. Suppose $\bar{S} \subseteq \overline{S_{even}}$ is δ-distributed. Then there exists an "Even" permutation σ so that $S(\sigma) \in \bar{S}$ and an "Odd" permutation so that to tell them apart with bounded probability requires $\Omega(N^{\delta/2})$ in-place queries
- Proof: new "Adversary bound for in-place oracles"
  - Adaptation of Ambainis original result for standard oracles
  - *Theorem*: Let $\boldsymbol{\sigma}$ be some subset of permutations acting on $[N^2]$.
    - Suppose f: $\boldsymbol{\sigma} \rightarrow \{0,1\}$, and let $\boldsymbol{\sigma}_{YES}$ be the set of permutations that f maps to 1, and $\boldsymbol{\sigma}_{NO}$ be the set of permutations that f maps to 0.
    - If $\exists$ R $\subset$ $\boldsymbol{\sigma}_{YES} \times \boldsymbol{\sigma}_{NO}$ so that:
      1. For every $\sigma_x \in \boldsymbol{\sigma}_{YES}$ there exists at least m different $\sigma_y \in \boldsymbol{\sigma}_{NO}$ so that $(\sigma_x, \sigma_y) \in R$
      2. For every $\sigma_y \in \boldsymbol{\sigma}_{NO}$ there exists at least m' different $\sigma_x \in \boldsymbol{\sigma}_{YES}$ so that $(\sigma_x, \sigma_y) \in R$
      3. Let $l_{x,i}$=number of different $\sigma_y \in \boldsymbol{\sigma}_{NO}$ so that $(\sigma_x, \sigma_y) \in R$ and $\sigma_x(i) \neq \sigma_y(i)$
      4. Let $l_{y,i}$=number of different $\sigma_x \in \boldsymbol{\sigma}_{YES}$ so that $(\sigma_x, \sigma_y) \in R$ and $\sigma_x(i) \neq \sigma_y(i)$
      5. $l_{max} = \max_{(\sigma x, \sigma y) \in R} l_{x,i} l_{y,I}$

    Then, given an in-place oracle P_σ any quantum algorithm that correctly evaluates f on all inputs with constant probability requires at least

    $\Omega\sqrt{\frac{mm'}{l_{max}}}$ in place queries to compute f(σ)

  - We'll use the δ-distributed property of the subset system to show an "R" relation so that the function f, which evaluates to 1 on "Even" σ so that $S(\sigma) \in \bar{S}$ and evaulates to 0 on "Odd" σ requires an exponential number of queries to compute.

A few open questions about **QMA**

- **QMA**$\not\subseteq$**QCMA** relative to a standard oracle?
  - Can this construction be extended?
- Unrelativized separations?
  - Seems to require new insights on entanglement structure of ground states of local Hamiltonians
- **QMA** vs **QMA**(2)
  - In **QMA**(2) Arthur receives tensor product of two pure quantum states on polynomial qubits
  - **QMA**$\subseteq$**QMA**(2) is trivial, but is **QMA**(2)$\subseteq$**QMA**?
    - Closely connected to “separability testing” and “quantum de Finetti theorems”

Thanks!