Space-Efficient Error Reduction for Unitary Quantum Computations

Bill Fefferman (QuICS), Hirotada Kobayashi (NII),
Cedric Yen-Yu Lin (QuICS), Tomoyuki Morimae (Gunma U.),
Harumichi Nishimura (Nagoya U.)

AQIS '16, Taipei
August 30, 2016

Overview

- Basic definitions
- Past work: QMA error reduction
- Our results

Basic definitions

Quantum time complexity

- A family of quantum circuits $\{V_x\}_{x \in \{0,1\}^n}$ acting on $k(n)$ qubits solves a promise problem $L = \left(L_{yes}, L_{no}\right)$ if

$$x \in L_{yes} \Rightarrow \left\langle 0^k \middle| V_x^{-1} |1\rangle\langle 1|_{out} V_x \middle| 0^k \right\rangle \geq 2/3$$

$$x \in L_{no} \Rightarrow \left\langle 0^k \middle| V_x^{-1} |1\rangle\langle 1|_{out} V_x \middle| 0^k \right\rangle \leq 1/3$$

- A problem is in BQTIME$[t(n)]$ if it is solved by a family* of circuits $\{V_x\}$ such that V_x uses at most $O\big(t(n)\big)$ gates.

E.g. BQP=$\bigcup_{t \in poly}$ BQTIME$[t(n)]$

*uniformly generated

Quantum space complexity

- A family of quantum circuits $\{V_x\}_{x\in\{0,1\}^n}$ acting on $k(n)$ qubits solves a promise problem $L = \left(L_{yes}, L_{no}\right)$ if

$$x \in L_{yes} \Rightarrow \left\langle 0^k \middle| V_x^{-1} |1\rangle\langle 1|_{out} V_x \middle| 0^k \right\rangle \geq 2/3$$

$$x \in L_{no} \;\; \Rightarrow \left\langle 0^k \middle| V_x^{-1} |1\rangle\langle 1|_{out} V_x \middle| 0^k \right\rangle \leq 1/3$$

- A problem is in BQSPACE$[k(n)]$ if it is solved by a family* of circuits $\{V_x\}$ such that V_x acts on at most $O\big(k(n)\big)$ qubits.
- Some subtleties in the definition; in our talk we demand that only unitary operations are allowed for V_x (no intermediate measurements)
  - Usual method of deferring measurements uses too much space

*uniformly generated

Quantum Merlin-Arthur (QMA)

- We consider problems that can be verified quantumly given a quantum witness.
- $k(n)$-bounded $\mathrm{QMA}_m(c,s)$ is the set of promise problems $L = (L_{yes}, L_{no})$ such that there is a circuit* acting on $m + O(k)$ qubits such that

$$x \in L_{yes} \Rightarrow \exists |\psi\rangle \in \mathbb{C}^m, \quad \left(\langle\psi|\langle 0^k|\right) V_x^{-1} |1\rangle\langle 1|_{out} V_x \left(|\psi\rangle|0^k\rangle\right) \geq c$$

$$x \in L_{no} \Rightarrow \forall |\psi\rangle \in \mathbb{C}^m, \quad \left(\langle\psi|\langle 0^k|\right) V_x^{-1} |1\rangle\langle 1|_{out} V_x \left(|\psi\rangle|0^k\rangle\right) \leq s$$

- QMA is a central class of study in quantum complexity, and many problems in physics are QMA–complete (e.g. Local Hamiltonian [Kitaev'02]).
- The focus of our talk is error reduction for space-bounded QMA.

*uniformly generated

Past work: QMA error reduction

Gap amplification for QMA

- Goal: Take a QMA(c, s) protocol and amplify it to a new protocol with completeness $c' > c$ and soundness $s' < s$
- Repetition [Kitaev '02]:
  - Our new witness is many copies of the original witness.
  - Perform original protocol on all copies, and accept or reject based on results.
  - To get 2^{-p} error, need $O(p/(c-s)^2)$ repetitions.

  - k-bounded $\mathrm{QMA}_m(c, s) \subseteq \left(k \cdot \frac{p}{(c-s)^2}\right)$–bounded $\mathrm{QMA}_{O\left(m \cdot \frac{p}{(c-s)^2}\right)}(1 - 2^{-p}, 2^{-p})$

  - Is there a way to reduce error without increasing the witness size?

In-place amplification [Marriott-Watrous '05]

- Define two projectors $\Delta = |0\rangle\langle 0|_{anc}$ and $\Pi = V_x^{-1}|1\rangle\langle 1|_{out}V_x$.

  The max success probability is the max eigenvalue of $\Delta\Pi\Delta$
- Verification procedure:
  - Initialize a state consisting of the witness and blank ancilla
  - Alternatingly measure $\{\Pi, I-\Pi\}$ and $\{\Delta, I-\Delta\}$, $O(p/(c-s)^2)$ times
  - Classical postprocessing of results: reject if consecutive measurements differ in results too many times
- Note that we don't require many copies of the witness!

  But still require $O(p/(c-s)^2)$ extra space to record intermediate results
- Result:

  k-bounded $\text{QMA}_m(c,s) \subseteq \left(k + \frac{p}{(c-s)^2}\right)$–bounded $\text{QMA}_m(1-2^{-p}, 2^{-p})$

Intuition for in-place amplification

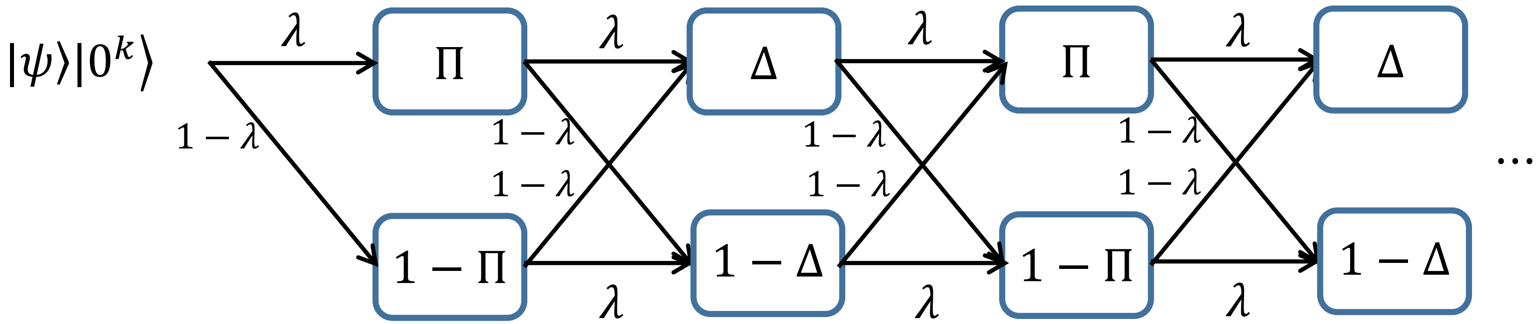
- Recall Jordan's lemma:

  Hilbert space decomposes into 1- and 2-dimensional subspaces invariant under Π and Δ.

- Assume starting state $|\psi\rangle|0^k\rangle$ is in one of these invariant subspaces.

  Let its original acceptance probability be λ.

  Measurements of Π and Δ never take the state out of invariant subspace:



Phase estimation approach [NWZ11]

- Phase estimation [Kitaev '95]:
  - Given unitary U and eigenstate ψ, estimates eigenvalue to precision j with failure prob. ε
  - Uses $O(\log(1/(j\varepsilon)))$ ancilla qubits and $O(1/(j\varepsilon))$ applications of controlled-U
  - Key ingredient in many q. algorithms, e.g. factoring [Shor94] and quantum counting [BHT98]
- Define rotations $R_0 = I - 2\Delta$ and $R_1 = I - 2\Pi$.

Then within each invariant subspace, $R_0 R_1$ is a rotation by an angle related to acceptance probability

- Apply p trials of phase estimation to $R_0 R_1$ to estimate max success probability.
  - Each trial performed to constant failure prob. and precision $O(c - s)$
  - Classical postprocessing on results
- Result: get space savings from use of phase estimation!

k-bounded $\mathrm{QMA}_m(c, s) \subseteq \left(k + p \log \frac{1}{c-s}\right)$–bounded $\mathrm{QMA}_m(1 - 2^{-p}, 2^{-p})$

Our results

Main thm: Space efficient QMA amplification

- Previous best result [NWZ11]:

$$k\text{-bounded } \mathrm{QMA}_m(c,s) \subseteq \left(k + p\log\frac{1}{c-s}\right)\text{–bounded } \mathrm{QMA}_m(1-2^{-p},2^{-p})$$

- To get error $2^{-\mathrm{poly}}$, requires polynomially many ancilla qubits.
- Our improved result:

$$k\text{-bounded } \mathrm{QMA}_m(c,s) \subseteq \left(k + \log\frac{p}{c-s}\right)\text{–bounded } \mathrm{QMA}_m(1-2^{-p},2^{-p})$$

- As a consequence, we obtain the first “strong error reduction” result for quantum logspace.

Main theorem (Proof sketch 1/3)

- I'll talk about the simplest proof we have.
- Suppose we have a verifier $\{V_x\}$ for k-bounded QMA$_m(c,s)$.

  We would like to reduce the error to 2^{-p}

1. Reduce error to $1/(8p)$ using phase estimation (à la [NWZ11])

   Let $V_x^{(1)}$ be the circuit that

   - Applies phase estimation to $R_0 R_1$ with precision $O(c-s)$ and failure prob. $1/(8p)$
   - Completeness = $1 - 1/(8p)$, soundness = $1/(8p)$
   - Uses space $O\left(k + \log \frac{1}{c-s} + \log p\right) = O\left(k + \log \frac{p}{c-s}\right)$

Main theorem (Proof sketch 2/3)

1. $V_x^{(1)}$ uses phase estimation to achieve completeness $1-1/(8p)$ and soundness = $1/(8p)$, using $O\left(k+\log\frac{p}{c-s}\right)$ space
2. Take the "AND" of $O(p)$ iterations of $V_x^{(1)}$

   Let $V_x^{(2)}$ be the circuit that implements the following:
   - Repeat $N_1 = O(p)$ times:
     - Apply $V_x^{(1)}$, and increments a counter if output state is accept
     - Apply $(V_x^{(1)})^{-1}$, and increments a counter if ancilla qubits not returned to 0
   - Accept iff counter remains 0.
   - Completeness $\geq 1-2N_1/(8p) \geq 1/2$, soundness = $(8p)^{-2N_1} \leq 2^{-O(p)}$
   - Only extra space used is for the counter, which takes $O(\log p)$ space

Main theorem (Proof sketch 3/3)

1. $V_x^{(1)}$ uses phase estimation to achieve completeness $1 - 1/(8p)$ and soundness = $1/(8p)$, using $O\left(k + \log \frac{p}{c-s}\right)$ space
2. $V_x^{(2)}$ takes "AND" of $O(p)$ iterations of $V_x^{(1)}$ to achieve constant completeness and exponentially small soundness
3. Take the "OR" of $N_2 = O(p)$ iterations of $V_x^{(2)}$
   - Repeat N_2 times:
     - Apply $V_x^{(2)}$, and increments a counter if output state is reject
     - Apply $(V_x^{(2)})^{-1}$, and increments a counter if ancilla qubits not returned to 0
   - Accept iff counter is at least 1.
   - Completeness $\geq 1 - 2^{-p}$, soundness $\leq 2^{-p}$

- Total space used: $O\left(k + \log \frac{p}{c-s}\right)$

Consequences (1/2)

- Strong error reduction for (unitary) quantum logspace:

  $\forall c - s > \frac{1}{\text{poly}}, \text{QSPACE}[\log(n)](c, s) \subseteq \text{QSPACE}[\log(n)](1 - 2^{-\text{poly}}, 2^{-\text{poly}})$

- Uselessness of quantum witnesses for space-bounded QMA
  - Idea: verifier can do error reduction, guess a random witness, and do error reduction again
  - Result: k-bounded $\text{QMA}_{O(k)}(2/3,1/3) = \text{BQSPACE}[k]$
- Strong error reduction for poly-sized nearest neighbor matchgate computations
  - Physically motivated model related to computation with noninteracting fermions
  - Equivalent to unitary quantum logspace [JKMW10]

Consequences (2/2)

- QMA with exponentially small gap is contained in PSPACE :

$$\text{PreciseQMA} \coloneqq \bigcup_{c-s>2^{-\mathrm{poly}}} \text{QMA}(c,s) \subseteq \text{PSPACE}$$

  - Uses the result that BQPSPACE = PSPACE [Watrous ‘00]
  - Turns out converse holds: PreciseQMA = PSPACE [Fefferman, L. ‘16]
    Computing ground state energy of a local Hamiltonian to poly digits is PSPACE-complete

Why unitary quantum space classes?

- Marriott-Watrous style in-place error reduction is only possible without intermediate measurements, since all such methods apply V_x^{-1}
  - For non-unitary quantum logspace, unknown how to reduce error to $o(1)$
  - In this case if $c - s = o(1)$, unknown how to reduce error to constant
- Unitary quantum logspace is equivalent to matchgate circuits [JKMW10]
- Natural complete problems for unitary quantum space classes [Fefferman, L. '16]

  e.g. for quantum logspace:
  - Computing minimum eigenvalue for Hermitian matrix
  - Computing inverse for well-conditioned matrix

  Analogous complete problems known for other unitary q. space classes
- Open question: do intermediate measurements give additional power?

Thanks!