Space-efficient Error Reduction for Unitary Quantum Computations

Bill Fefferman

QuICS, University of Maryland/NIST

Joint with Hirotada Kobayashi, Cedric Yen-Yu Lin, Tomoyuki Morimae, and Harumichi Nishimura

ICALP 2016

Overview

1. Basic Definitions
2. Past work: **QMA** error amplification
3. Our results

1. Basic Definitions

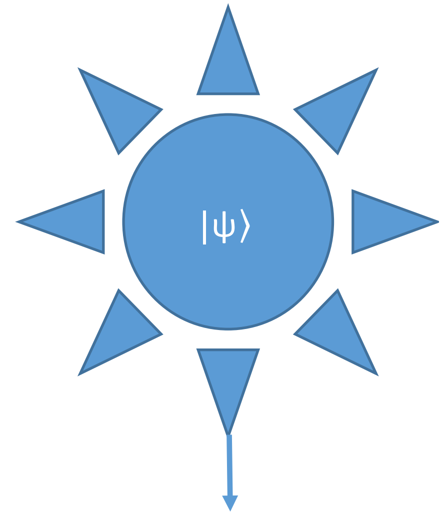
Unitary quantum space complexity

- We say that a family of quantum circuits $\{Q_x\}_{x \in \{0,1\}^n}$ acting on k(n) qubits *solves* a promise problem $L=(L_{yes},L_{no})$ if:

$$x \in L_{yes} \Rightarrow \langle 0^k | Q_x^\dagger |1\rangle\langle 1|_{out} Q_x | 0^k \rangle \geq 2/3$$
$$x \in L_{no} \Rightarrow \langle 0^k | Q_x^\dagger |1\rangle\langle 1|_{out} Q_x | 0^k \rangle \leq 1/3$$

- **BQTIME**[t(n)] is the class of promise problems solvable in quantum *time* t(n):
  - i.e., by a uniformly generated family of quantum circuits $\{Q_x\}$, each composed of O(t(n)) gates
- **BQSPACE**[k(n)] is the class of promise problems solvable in k(n) quantum *space*
  - i.e., by a uniformly generated family of quantum circuits $\{Q_x\}$ each acting on O(k(n)) qubits
- Subtleties in defining quantum space bounded computation
  - Power of intermediate measurements?
  - Our focus: *unitary* case

Quantum Merlin-Arthur



- Problems whose solutions can be verified quantumly given a quantum state as witness
- k(n)-**bounded QMA**$_m$(c,s) is the class of promise problems $L=(L_{yes},L_{no})$ so that there exists a verifier $\{V_x\}$ acting on $O(m(|x|)+k(|x|))$ qubits:

$$x \in L_{yes} \Rightarrow \exists|\psi\rangle \ \left(\langle\psi| \otimes \langle 0^k|\right) V_x^\dagger |1\rangle\langle 1|_{out} V_x \left(|\psi\rangle \otimes |0^k\rangle\right) \geq c$$

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

- **QMA** is a central topic of study in quantum complexity theory
  - "Quantum **NP**"
  - Many connections to physics (i.e., estimating the ground state energy of a Local Hamiltonian is **QMA**-complete [Kitaev'02])
  - But some of the most natural questions are embarrassingly open
  - Our main result is a method for *space-efficient* **QMA** *error-amplification*

2. Past work: QMA error amplification

QMA error amplification using repetition

- "Repetition" [Kitaev '02]
  - Ask Merlin to send many copies of the original witness
  - Verifier repeats original protocol on each one, measures and takes majority vote of outcomes
  - Using Chernoff bound, to obtain error 2^{-p}, need $O(p/(c-s)^2)$ repetitions
  - *Problem with this*: number of witness and space qubits grow with improving error bounds
  - i.e., for any given p:

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

“In-place” QMA amplification

- “Amplification without destroying witness” [Marriott and Watrous ’04]
  - Define two projectors: $\Pi_0 = |0\rangle\langle 0|_{anc}$ and $\Pi_1 = V_x^\dagger |1\rangle\langle 1|_{out} V_x$
  - Notice the max. acceptance probability of V_x is the maximal eigenvalue of $\Pi_0 \Pi_1 \Pi_0$
  - Verification procedure:
    - Initialize a state consisting of Merlin’s witness tensored with ancilla qubits initialized to all-zero state
    - Alternatingly measure $\{\Pi_0, 1-\Pi_0\}$ and $\{\Pi_1, 1-\Pi_1\}$ many times
  - Use post processing to analyze results of measurements (rejecting if two consecutive measurement outcomes differ too many times)
- Analysis relies on “Jordan’s lemma”
  - Given two projectors, Hilbert space decomposes into 1 and 2-dimensional subspaces invariant under projectors
  - Basically allows verifier to repeat each measurement without “losing” Merlin’s witness
    - Because application of these projectors “stays” inside 2D subspaces
  - As a result, we can attain the same type of error reduction as in repetition, without needing additional witness qubits
  - However, we need additional space to keep track of measurement outcomes

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

3. Our results

Our results: Space-efficient QMA error amplification

- Nagaj, Wocjan, and Zhang [NWZ'11] improvements on Marriott-Watrous:

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

- Notice to achieve error $2^{\text{-poly}}$ requires polynomial extra ancilla qubits!
- ***Main Theorem***:

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

- As a consequence, we show the first "strong" error amplification procedure for unitary quantum logspace protocols
- We give three proofs of main theorem using different procedures
  - I'll talk about the simplest one
  - Other two proofs achieve better parameters

Main Theorem (Proof sketch 1/3)

- We'll use the phase estimation algorithm [Kitaev '95]
  - Important ingredient in many quantum algorithms
  - Given quantum circuit for implementing unitary U and eigenvector $|\psi>$ estimates eigenphase θ
    - Up to precision *j* with failure probability α using <u>O(*log(1/j*α*))* ancilla qubits</u>
- Define reflections $R_0 = 2\Pi_0 - I, R_1 = 2\Pi_1 - I$
    - These are the "Grover" reflections that apply a phase flip if not in the projected subspace
- Using Jordan's lemma:
  - Within 2D subspaces, the product R_0R_1 is a rotation by an angle related to acceptance probability of verifier V_x

1. Use phase estimation on R_0R_1 with Merlin's state and ancillias set to 0, to amplify error to inverse polynomial (related to approach of [NWZ'11])
   - Accept if phase is above a certain threshold, reject otherwise
   - Do this with precision O(c-s) and failure probability α=1/(8p)
   - Completeness is 1-1/(8p), Soundness is 1/(8p)
   - Uses space O(log(p/(c-s)))

Main Theorem (Proof sketch 2/3)

1. $V_x^{(1)}$ runs mild phase estimation to achieve completeness $1-1/(8p(n))$ and soundness $1/(8p(n))$
2. Take "AND" of $N_1=O(p(n))$ iterations of $V_x^{(1)}$
   - Let $V_x^{(2)}$ be the quantum circuit repeats the following N_1 times:
     - Applies $V_x^{(1)}$ and increments a counter if the output state is reject
     - Applies $(V_x^{(1)})^\dagger$
   - Accept iff counter is still set to 0
   - Completeness is $1-N_1/8p(n)\geq 1/2$, Soundness is $(1/(8p(n)))^{N_1}\leq 2^{-p(n)}$

Main Theorem (Proof sketch 3/3)

1. $V_x^{(1)}$ runs mild phase estimation to achieve completeness 1-1/(8p(n)) and soundness 1/(8p(n))
2. $V_x^{(2)}$ takes "AND" of N_1 iterations of $V_x^{(1)}$ to achieve constant completeness, and exponentially small soundness error
3. Take "OR" of $N_2=O(p(n))$ iterations of $V_x^{(2)}$
   - Repeats the following N_2 times:
     - Applies $V_x^{(2)}$ and increments a counter by 1 if the output state is accept
     - Applies $(V_x^{(2)})^\dagger$
   - Accept iff counter is at least 1
   - Completeness is at least $1-2^{-p(n)}$, Soundness is at most $p(n)2^{-p(n)}$

- *Key point*: The space used in the new verification procedure is $O(\log(p/(c-s)))+\log(N_1)+\log(N_2)=O(\log(p/(c-s)))$
- Other proofs achieve similar amplification results without phase estimation

Applications of Main Theorem

- Strong error reduction for unitary quantum logspace
  - i.e., for any $a\text{-}b \geq 1/\text{poly}$, **QSPACE**[log(n)](a,b)$\subseteq$ **QSPACE**[log(n)]($1\text{-}2^{\text{-poly}}, 2^{\text{-poly}}$)
- Uselessness of quantum witnesses in log(n)-**bounded QMA**
  - *Idea*: Logspace algorithm with no witness can choose random log(n) bit basis state as witness, and then error amplify
  - i.e., log(n)-**bounded** $\textbf{QMA}_{\log(n)}$(2/3,1/3)=**BQSPACE**[log(n)]
- **QMA** with exponentially small completeness-soundness gap is contained in **PSPACE**
  - i.e., **PreciseQMA**$\subseteq$**PSPACE**
  - Proofs use Main theorem and "uselessness of quantum witness in log(n)-**bounded QMA**"
  - Has several applications to physics via Local Hamiltonian problem
- Strong error amplification of Matchgate computations
  - Physically motivated model (related to quantum computation with *noninteracting fermions*)
  - Known to be classically simulable [Valiant '02]
  - Uses equivalence of logspace quantum computation and matchgate computation [Jozsa et. al. '10]

A Complete Characterization of Unitary Quantum Space [F., Lin '16]

- Why are we interested in *unitary* quantum space complexity?
- Motivated by recent result [F., Lin '16]
  - Gives two natural complete problems for (unitary) **BQSPACE**[k(n)]
    - Under classical k(n)-space poly(n)-time reductions
    - Given a succinctly specified $2^{k(n)}$x $2^{k(n)}$ PSD matrix A:
      1. Estimate a given entry of A^{-1} (assuming A is *well-conditioned*)
      2. Estimating minimum eigenvalue of A to inverse exponential precision
    - Interestingly, the Matrix inversion problem with different parameter setting is complete for **BQTIME**[t(n)] as well
- As a corollary, we can show the lowerbound **PSPACE**$\subseteq$**preciseQMA**
  - And so together with upperbound from today's results, **preciseQMA**=**PSPACE**
- For more details see *arXiv:1604.01384*

Open Questions

- Can we find space-efficient methods for in-place amplification of **QMA** *with* intermediate measurements?
  - Note that Marriott-Watrous projection operators explicitly use the inverse of the verification procedure
- What is the power of **QMA** with doubly-exponentially small gap?
  - Can show that this is still equal to **PSPACE** if protocol has perfect completeness
- Can we use this upperbound on **preciseQMA** to show upper bounds for other complexity classes?

Thanks!