A Complete Characterization of Unitary Quantum Space

Bill Fefferman (QuICS, University of Maryland/NIST)

Joint with Cedric Lin (QuICS)

Based on arxiv:1604.01384

1. Basics

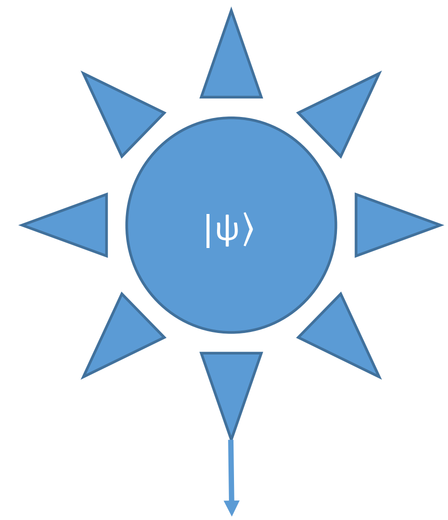
Quantum space complexity

- *Main result*: Give two problems "*characterize*" unitary quantum space complexity
  - *Roughly*: What problems can we solve by quantum computation with a bounded number of qubits?
  - For all space bounds log(n)≤k(n)≤poly(n) we find a **BQSPACE**[k(n)]-complete problem
  - Our reductions will use *classical* poly(n) time and O(k(n))-space
  - What is *classical* k(n)-space/memory?
    - Input is on its own "read-only" tape, doesn't use space
    - Each bit of the output can be computed in O(k(n))-space
  - k(n)-Precise Succinct Hamiltonian and k(n)-Well-Conditioned Matrix Inversion
- **BQSPACE**[k(n)] is the class of promise problems $L=(L_{yes},L_{no})$ solvable with a bounded error quantum algorithm acting on O(k(n)) qubits:
  - Exists uniformly generated family of quantum circuits $\{Q_x\}_{x\in\{0,1\}^*}$ each acting on O(k(|x|)) qubits:
  - "If answer is yes, the circuit Q_x accepts with high probability"
    $x \in L_{yes} \Rightarrow \langle 0^k|Q_x^\dagger|1\rangle\langle 1|_{out}Q_x|0^k\rangle \geq 2/3$
  - "If answer is no, the circuit Q_x accepts with low probability"
    $x \in L_{no} \Rightarrow \langle 0^k|Q_x^\dagger|1\rangle\langle 1|_{out}Q_x|0^k\rangle \leq 1/3$
  - **Uniformly generated* means poly-time, O(k)-space

Known (and unknown) in space complexity

- Any $k \geq \log(n)$, **NSPACE**[$k(n)$]$\subseteq$**DSPACE**[$k(n)^2$] [Savitch '70]
  - Via algorithm for directed graph connectivity, with n vertices in $\log^2(n)$ space
  - (Obvious) Corollary 1: **NPSPACE**=**PSPACE**
  - (Obvious) Corollary 2: **NL**=**NSPACE**[$\log(n)$]$\subseteq$**DSPACE**[$\log^2(n)$]
- Undirected Graph Connectivity with n vertices is complete for **DSPACE**[$\log(n)$]=**L** [Reingold '05]
- **BQSPACE**[$k(n)$]$\subseteq$**DSPACE**[$k(n)^2$] [Watrous'99]
  - In particular, **BQPSPACE**=**PSPACE**
- Well-conditioned Matrix inversion in non-unitary quantum space $\log(n)$ [Ta-Shma'14] building on [HHL'08]
- What is the power of intermediate measurements in quantum logspace?
  - Note that "deferring" measurements in the standard sense is not space efficient
    - i.e., a quantum logspace algorithm could make as many as $\mathrm{poly}(n)$ measurements
    - Deferring the measurements requires $\mathrm{poly}(n)$ ancilla qubits

Quantum Merlin-Arthur



- Problems whose solutions can be verified quantumly given a quantum state as witness
- (**t(n)**,**k(n)**)-**bounded QMA$_{\mathbf{m}}$**(**a**,**b**) is the class of promise problems L=(L$_{yes}$,L$_{no}$) so that:

$$x \in L_{yes} \Rightarrow \exists|\psi\rangle \ \Pr[V(x,|\psi\rangle)=1] \geq a$$

$$x \in L_{no} \Rightarrow \forall|\psi\rangle \ \Pr[V(x,|\psi\rangle)=1] \leq b$$

  - Where V runs in quantum time t(n), and quantum space k(n)
  - And the witness, |Ψ> is an m qubit state
- **QMA**=(poly,poly)-**bounded QMA$_{\mathbf{poly}}$**(2/3,1/3)=(poly,poly)-**bounded** $\bigcup_{c>0}$**QMA$_{\mathbf{poly}}$**(c,c-1/poly)
- **preciseQMA**=(poly,poly)-**bounded** $\bigcup_{c>0}$**QMA$_{\mathbf{poly}}$** (c,c-1/exp)
- *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* $\langle\psi|H|\psi\rangle \leq a$
    - $\forall\,|\psi\rangle$ *so that* $\langle\psi|H|\psi\rangle \geq b$

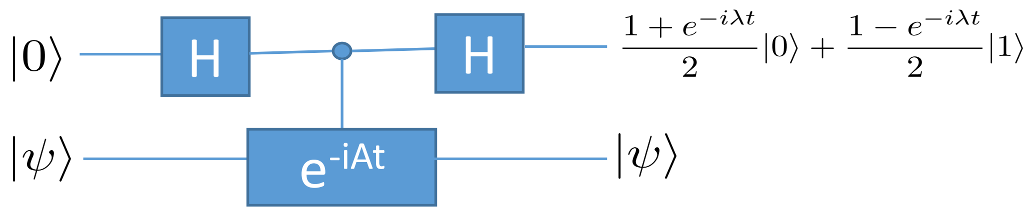
2. Characterization 1: $k(n)$-*Precise Succinct Hamiltonian problem*

Definitions and proof overview

- Definition: *Succinct encoding*
  - Let A be a $2^{k(n)}$ x $2^{k(n)}$ matrix.
  - We say a classical Turing Machine M is a *succinct encoding* for matrix A if:
    - On input $i \in \{0,1\}^{k(n)}$, M outputs non-zero elements in i-th row of A
    - In poly(n) time and k(n) space
- k(n)-*Precise Succinct Hamiltonian Problem*
  - Input: Size n succinct encoding of $2^{k(n)}$ x $2^{k(n)}$ PSD matrix A so that:
    - $|H|=\max_{s,t}(A(s,t))$ is constant
    - Promised minimum eigenvalue is either greater than b or less than a, where $b-a>2^{-O(k(n))}$
  - Which is the case?
- Proof Sketch of **BQSPACE**[k(n)]-completeness (details in next slides)
  - *Upper bound*: k(n)-*P.S Hamiltonian Problem* $\in$ **BQSPACE**[k(n)]
  1. k(n)-*P.S Hamiltonian Problem* $\in$ (poly,k(n))-**bounded QMA**$(c,c-2^{-k(n)})$
     - **preciseQMA** with k(n)-space bounded verifier
  2. (poly,k(n))-**bounded QMA**$(c,c-2^{-k(n)})$ $\subseteq$ **BQSPACE**[k(n)]
  - *Lower bound*: **BQSPACE**[k(n)]-hardness
    - Application of Kitaev's clock-construction

Upper bound (1/4): k(n)-*P.S Ham.* $\in$ (poly,k(n))-bounded QMA$_{k(n)}$(c,c-$2^{-k(n)}$)

- Recall: k(n)-Precise Succinct Hamiltonian problem
  - Given succinct encoding of $2^{k(n)}$ x $2^{k(n)}$ matrix A, is $\lambda_{min} \geq$ b or $\leq$ a where b-a$\geq 2^{-O(k(n))}$?
- Ask Merlin to send eigenstate $|\psi\rangle$ with minimum eigenvalue
  - Arthur runs the "poor man's phase estimation" circuit on e^{-iAt} and $|\psi\rangle$



  - Measure ancilla and accept iff "0"
  - *First assume e^{-iAt} can be implemented exactly*
  - Easy to see that we get "0" outcome with probability that's slightly ($2^{-O(k)}$) higher if λ_{min} < a than if λ_{min} > b
  - But this is exactly what's needed to establish the claimed bound!
- Can use high-precision sparse Hamiltonian simulation of [Childs et. al.'14] to implement e^{-iAt} to within precision ε in time and space that scales with log(1/ε)
  - We'll need to implement up to precision $\varepsilon=2^{-k(n)}$
- This circuit uses poly(n) time and O(k(n)) space

Upper bound (2/4): QMA amplification

- We have shown that k(n)-*Precise Succinct Hamiltonian* is in k(n)-space-bounded **preciseQMA**
- *Next step*: apply space-efficient "in-place" **QMA** amplification to our **preciseQMA** protocol
- How do we error amplify **QMA**?
  1. "Repetition" [Kitaev '99]
     - Ask Merlin to send many copies of the original witness and run protocol on each one, take majority vote
     - *Problem with this*: number of proof qubits grows with improving error bounds
     - Needs $r/(c-s)^2$ repetitions to obtain error 2^{-r} by Chernoff bound
  2. "In-place" [Marriott and Watrous '04]
     - Define two projectors: $\Pi_0 = |0\rangle\langle 0|_{anc}$ and $\Pi_1 = V^\dagger |1\rangle\langle 1|_{out} V$
     - Notice that the max. acceptance probability of the verifier is maximal eigenvalue of $\Pi_0 \Pi_1 \Pi_0$
     - Procedure
       - Initialize a state consisting of Merlin's witness and blank ancilla
       - 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, there's an orthogonal decomposition of the Hilbert space 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

For many other space-efficient **QMA** amplification techniques, see [F., Kobayashi, Lin, Morimae, Nishimura **arXiv:1604.08192, ICALP'16**]

Upper bound (3/4): Space-efficient In-place amplification

- We're not happy with Marriott-Watrous amplification!!
  - M-W: $k-\text{bounded QMA}_m(c,s) \subseteq (k+\frac{r}{(c-s)^2})-\text{bounded QMA}_m(1-2^{-r},2^{-r})$
  - The space grows because we need to keep track of each measurement outcome
  - For our application we really want to be able to *space-efficiently* amplify protocol with inverse exponentially small (*in k*) gap
    - Recall: our parameters: log(n)≤k≤poly(n), c-s=$1/2^k$ and r=k
    - Then using MW the space complexity in amplified protocol is far larger than k
- We are able to improve this!

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

  - Now the same setting of parameters preserves O(k) space complexity!
  - Proof idea:
    - Define reflections $R_0 = 2\Pi_0 - I, R_1 = 2\Pi_1 - I$
    - 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
    - Use phase estimation on R_0R_1 with Merlin's state and ancillias set to 0
      - Key point: Phase estimation to precision *j* with failure probability α uses O(*log(1/jα)*) ancilla qubits
    - "Succeed" if the phase is larger than fixed threshold, reject otherwise
    - Repeat this many times and use classical post-processing on the outcomes to determine acceptance
  - Related to older result of [NWZ'11] but improves on space complexity

Upper bound (4/4): (poly,k(n))-bounded $\mathrm{QMA}_{k(n)}(c,c-2^{k(n)}) \subseteq \mathrm{BQSPACE}[k(n)]$

- Recall: $(t,k)\text{-}bounded\ \mathsf{QMA}_\mathsf{m}(\mathsf{c},\mathsf{s}) \subseteq (\mathcal{O}\left(\frac{\mathsf{tr}}{\mathsf{c}-\mathsf{s}}\right), \mathcal{O}\left(\mathsf{k}+\log\left(\frac{\mathsf{r}}{\mathsf{c}-\mathsf{s}}\right)\right))\text{-}bounded\ \mathsf{QMA}_\mathsf{m}(1-2^{-\mathsf{r}},2^{-\mathsf{r}})$
- Applying this amplification result:
  - (poly,k(n))-**bounded** $\mathbf{QMA}_k(c,c-2^{-k(n)}) \subseteq (2^{O(k)},k(n))$-**bounded** $\mathbf{QMA}_k(1-2^{-O(k)},2^{-O(k)})$
- Removing the witness! [Marriott and Watrous '04]
  - *Thm. RHS* $\subseteq$ **QSPACE**$[O(k)](3/4(2^{-O(k)}),1/4(2^{-O(k)}))$
    - *Pf. Idea*: Consider the same verification procedure that uses randomly chosen basis state for a witness
- But now we can use our amplification result again (with m=0)!
  - *RHS* $\subseteq$ **BQSPACE**$[O(k)]$

Lower bound: $k(n)$-*Precise Succinct Hamiltonian* is **BQSPACE**[$k(n)$]-hard

- An easy corollary of our "space-efficient" amplification together with Kitaev's clock construction
- Let $L=(L_{yes},L_{no})$ be any problem in **BQSPACE**[$k(n)$]
- By definition L is decided by uniform family of bounded error quantum circuits using $k(n)$ space
  - wlog circuit is of size at most $2^{k(n)}$
- Space-efficiently amplify this circuit (without changing the size or space too much)
- Kitaev shows how to take this circuit and produce a Hamiltonian with the property that:
  - In the "yes case", the Hamiltonian's minimum eigenvalue is less than some quantity involving the *completeness* and the circuit size
  - In the "no case", the Hamiltonian's minimum eigenvalue is at least some quantity involving the *soundness* and the circuit size
- By amplifying the completeness and soundness of the circuit we can ensure that the promise gap of the Hamiltonian is at least 2^{-k}
- Easy to show that this Hamiltonian is succinctly encoded
  - Follows from sparsity of Kitaev's construction and uniformity of circuit

Application 1: **preciseQMA=PSPACE**

- *Question:* How does the power of **QMA** scale with the completeness-soundness gap?
- *Recall*: **preciseQMA**=$\mathrm{U}_{c>0}$**QMA**($c,c\text{-}2^{-\mathrm{poly}(n)}$)
- Upper bound: **preciseQMA**$\subseteq$**BQPSPACE**=**PSPACE**
  - Prior slides showed something stronger!
- Lower bound: **PSPACE**$\subseteq$**preciseQMA**
  - We just showed k(n)-*Precise Succinct Hamiltonian Problem* is **BQSPACE**[k(n)]-hard
  - Since **BQPSPACE**=**PSPACE** [Watrous'03] we have poly(n)-*Precise Succinct Hamiltonian Problem* is **PSPACE**-hard

Application 1: preciseQMA=PSPACE

- Could **QMA=preciseQMA=PSPACE**?
  - Unlikely since **QMA=preciseQMA** $\Rightarrow$ **PSPACE=PP**
    - Using **QMA** $\subseteq$ **PP**
- What is the classical analogue of **preciseQMA**?
  - Certainly $\mathbf{NP}^{\mathbf{PP}} \subseteq \mathbf{PP}^{\mathbf{PP}} \subseteq$ **PSPACE**
  - $\mathbf{PP}^{\mathbf{PP}}$=**PSPACE** $\Rightarrow$**CH** collapse!
- *Corollary*: "precise k-Local Hamiltonian problem" is **PSPACE**-complete
- *Extension: "Perfect Completeness"*: **QMA**($1,1-2^{-poly(n)}$)=**PSPACE**
  - *Corollary:* checking if a local Hamiltonian has zero ground state energy is **PSPACE-**complete

Application 2:Preparing **PEPS** vs **Local Hamiltonian**

- Two boxes:
  - $\mathcal{O}_{\text{PEPS}}$: Takes as input classical description of **PEPS** and outputs the state
  - $\mathcal{O}_{\text{Local Hamiltonian}}$: Takes as input classical description of Local Hamiltonian and outputs the ground state
- We show a setting in which $\mathcal{O}_{\text{Local Hamiltonian}}$ is more powerful than $\mathcal{O}_{\text{PEPS}}$
- **$\mathbf{BQP}^{\mathcal{O}_{\text{PEPS}}}$=PostBQP=PP** [Schuch et. al.'07]
  - Can extend proof to show this is also true with unbounded error
  - i.e., **$\mathbf{PQP}^{\mathcal{O}_{\text{PEPS}}}$=PP**
- How powerful is **$\mathbf{PQP}^{\mathcal{O}_{\text{Local Hamiltonian}}}$**?
  - **PSPACE=PreciseQMA** $\subseteq$ **$\mathbf{PQP}^{\mathcal{O}_{\text{Local Hamiltonian}}}$**
- So $\mathcal{O}_{\text{Local Hamiltonian}}$ is more powerful unless **PP=PSPACE**

3. Characterization 2: $k(n)$-Well Conditioned Matrix Inversion

Our results on Matrix Inversion

- Classically, we know that n x n Matrix Inversion is in $\log^2(n)$ space, but don't believe it can be solved in *classical* $\log(n)$ space
- $k(n)$-*Well-conditioned Matrix Inversion*
  - Input: Efficient encoding of 2^k x 2^k PSD matrix A, and $s,t \in \{0,1\}^k$:
    - Upper bound $\kappa < 2^{O(k(n))}$ on the condition number so that $\kappa^{-1} I \prec A \prec I$
    - Promised either $|A^{-1}(s,t)| \geq b$ or $\leq a$ where a,b are constants between 0 and 1
  - Decide which is the case?
- *Our result:* $k(n)$-*Well-conditioned Matrix Inversion* is complete for **BQSPACE**[k(n)]
- Improves on Ta-Shma:
  1. No intermediate measurements!
  2. We also have hardness!
- Complexity implications:
  - If Matrix inversion can be solved in **L** then **BQL**=**L** (seems unlikely)
  - Evidence of quantum space hierarchy theorem?
    - k(n)-Well-conditioned Matrix inversion seems strictly harder with larger k
    - Seems close to showing if $f(n)=o(g(n))$ then **BQSPACE**[$g(n)$]$\not\subset$**BQSPACE**[$f(n)$]

Thanks!