Reducing Error Probabilities of Quantum Merlin-Arthur Proof Systems

Harumichi Nishimura
Nagoya University

September 17, 2012
Japan-Singapore Workshop on multi-user quantum networks
QMA Proof Systems

Prover (Merlin) unbounded powerful

Verifier (Arthur) p-time quantum algorithm

$L \in \text{QMA}(a,b)$

There is a p-time quantum algorithm $V$ such that:

(completeness) If $x$ is in $L$, there is a state $|\varphi\rangle$ such that $V$ accepts with probability at least $a$;

(soundness) If $x$ is not in $L$, for any $|\varphi\rangle$ the probability that $V$ accepts is at most $b$.

$1 - a := \text{completeness error}$

$b := \text{soundness error}$

$a - b := \text{completeness-soundness gap}$
This Talk

• Many variants of QMA
  • QCMA: proof is classical [AN02]
  • QMA[k]: multiple provers [KMY03]
  • QMA_{log}: proof-length is logarithmic [MW05]

• Amplifying completeness-soundness gap
  • Improvement of the completeness-soundness gap for QMA[2] with log-length quantum proofs (joint work with F. Le Gall and S. Nakagawa)

• Converting two-sided error to one-sided error
  • QCMA equals the one-sided error subclass QCMA_1 (joint work with S. P. Jordan, H. Kobayashi and D. Nagaj)
Amplifying completeness-soundness gap
There is a p-time quantum algorithm $V$ such that:

- (completeness) If $x$ is in $L$, there is a state $\ket{\varphi_1} \otimes \ket{\varphi_2}$ such that $V$ accepts with probability at least $a$;
- (soundness) If $x$ is not in $L$, for any $\ket{\varphi_1} \otimes \ket{\varphi_2}$ the probability that $V$ accepts is at most $b$. 

$L \in \text{QMA}[2]_{\log}(a,b)$
Why $\text{QMA}[2]_{\log}$

- NP-complete problems are in $\text{QMA}[2]_{\log}(1,1-1/poly)$. [BT09]
  - completeness-soundness gap is only $1/poly$, but;
  - $\text{QMA}_{\log}(1,1-1/poly)$ has only the languages recognized by $p$-time quantum algorithms with exponentially small error [MW05]; so
- $\text{QMA}[2]_{\log}$ indicates that two disentangled quantum proofs may be helpful for QMA proof systems.
- Can we improve the completeness-soundness gap?
  - this question is “currently” specific for $\text{QMA}[2]_{\log}$ because the completeness/soundness errors of other variants can be exponentially reduced;
    - $\text{QMA}=\text{QMA}(1-1/exp,1/exp)$ [KSV02,AN02]
    - $\text{QMA}_{\log}=\text{QMA}_{\log}(1-1/exp,1/exp)$ [MW05]
    - $\text{QMA}[2]=\text{QMA}[2](1-1/exp,1/exp)$ [HM10]
Previous & Our Works

• **Previous Works**
  - 3-COLORING is in QMA[2]_{log}(1,1-1/n^6). [BT09]
  - The gap was improved to 1/n^{3+\varepsilon} for 3-SAT [Bei10]
    - completely different protocol from [BT09]
    - completeness error is not 0
  - 1/n^2 [CF11,NN10]
    - same protocol as [BT09]
    - further improvement is impossible as long as the [BT09] protocol is used.

• **Our Work & Implication** [LNN12]
  - 1/n*\log\text{poly}(n)
    - combines the [BT09] protocol with Dinur’s PCP reduction [Din07,CD10]
    - needs a different analysis from [BT09]
  - NP-hard to estimate $h_{\text{sep}}(M) = \max \text{tr } M(\alpha \otimes \beta)$ where the maximum is taken over two d-dimensional states $|\alpha\rangle$, $|\beta\rangle$ with accuracy $1/d^*\log\text{poly}(d)$ (see [HM10,BBH+12])
Problem: 3COL
Input: a graph $G = (V, E)$; Output: Yes iff there is a mapping $c$ from $V$ to \{0,1,2\} such that for any $(i, i') \in E$, $c(i) \neq c(i')$

Ideal states: $|\varphi_1\rangle = |\varphi_2\rangle = \frac{1}{\sqrt{n}} \sum_i |i\rangle |c(i)\rangle$

Protocol: Given $|\varphi_1\rangle$ from Prover1 & $|\varphi_2\rangle$ from Prover2
Perform one of the following tests with equal prob.

(Equality) Do the swap test on $|\varphi_1\rangle \otimes |\varphi_2\rangle$
REJECT if the test outputs NO.

(Consistency) Measure $|\varphi_1\rangle$ and $|\varphi_2\rangle$ in the computational basis, yielding the outcomes $(i, j)$ and $(i', j')$. Then:
  a) if $i = i'$, REJECT if $j \neq j'$.
  b) if $i \neq i'$ and $(i, i') \in E$, REJECT if $c(i) = c(i')$.

(Uniformity) For both $|\varphi_1\rangle$ and $|\varphi_2\rangle$
the Fourier transform $F_3$ is applied on the color register, which is then measured in the comp. basis. If the outcome is 0, $F_3^{-1}$ is applied on the vertex register, which is then measured in the comp. basis. REJECT if the 2nd outcome is not 0.

ACCEPT
Soundness of [BT09] Protocol

$G$ might have a coloring $c'$ such that only one edge $(u, v)$ fails (i.e., they have the same color). Then malicious provers can send

$$|\varphi_1\rangle = |\varphi_2\rangle = \frac{1}{\sqrt{n}} \sum_i |i\rangle |c'(i)\rangle$$

**Protocol:** Given $|\varphi_1\rangle$ from Prover1 & $|\varphi_2\rangle$ from Prover2

Perform one of the following tests with equal prob.

(Equality) Do the swap test on $|\varphi_1\rangle \otimes |\varphi_2\rangle$

\[\text{REJECT if the test outputs NO.}\]

(Consistency) Measure $|\varphi_1\rangle$ and $|\varphi_2\rangle$ in the computational basis, yielding the outcomes $(i, j)$ and $(i', j')$. Then:

a) if $i = i'$, \text{REJECT if } j \neq j'$.

b) if $i \neq i'$ and $(i, i') \in E$, \text{REJECT if } c(i) = c(i').

(Uniformity) For both $|\varphi_1\rangle$ and $|\varphi_2\rangle$ the Fourier transform $F_3$ is applied on the color register, which is then measured in the comp. basis. If the outcome are

\[i = u, i' = v \text{ with probability only } 1/n^2\]

\text{ACCEPT}
Towards Gap $1/n^{*}\text{polylog}(n)$

- Use a problem such that for any NO instance, any coloring “fails” for a constant fraction of edges.
- Such a “promise” problem (so-called GAP-CSP) is obtained by the excellent classical result – Dinur’s PCP reduction [Din07,CD10].
- Our analysis is tight, which means that for some NO instance, malicious provers can make the verifier accept with prob. $1 - \Omega(1/n)$ in our protocol.

Our problem: 3SAT
Is there a Boolean assignment satisfying a given 3CNF formula?

[BT09] Protocol
Converting two-sided error to one-sided error
Why One-sided Error

• A (verification) protocol for a language $L$ is one-sided or has perfect completeness (resp., two-sided) if it:
  • always accepts (resp., with high prob.) if the input is in $L$;
  • rejects with high prob. if the input is not in $L$.
• Merits of One-Sided Error
  • In an ideal proof system, any honest prover should be always accepted by the verifier.
  • One-sided error is simpler to analyze than two-sided-error. It is good for showing deep results, say,  
    • quantum interactive proof systems [KW00]
    • multi-prover QIP systems [KKMV09]
QMA vs. QMA₁

- \( \text{QMA}_1 := \text{QMA}(1, 1/2); \ \text{QMA} := \text{QMA}(2/3, 1/3); \)
  - The errors of both classes can be exponentially reduced
- \( \text{QMA} = \text{QMA}_1? \)
  - In the classical case, MA = MA₁ [ZF87]
  - If the answer is positive, any QMA-complete problem such as Local Hamiltonian can be reduced to QSAT, which is QMA₁-complete [Bra06]
  - There is a negative result for the equality; the existence of a “quantum” oracle that separates between the two classes [Aar09]
  - Remains open for many years
- What if a well-studied QMA variant, QCMA, which is between QMA and MA?
There is a p-time quantum algorithm $V$ such that:

- **(completeness)** If $x$ is in $L$, there is a bit-string $\gamma$ such that $V$ accepts with probability at least $a$;
- **(soundness)** If $x$ is not in $L$, for any $\gamma$ the probability that $V$ accepts is at most $b$.

$L \in QCMA(a,b)$ if and only if $x \in L$?

**QCMA**

$QCMA_1 := QCMA(1,1/2); QCMA := QCMA(2/3,1/3)$
Our Result & Implication

- **Result**: QCMA=QCMA$_1$ [JKNN12]
  - rigorously, it holds under any gate set with which the Hadamard and arbitrary classical reversible gates can be exactly implemented, say, \{H,Toffoli,NOT\}
  - completely different proof from MA=MA$_1$
  - simple but novel technique that “additively” adjusts the success prob.

- **Implication**
  - the “quantum” oracle result of [Aar09] may not be an insurmountable barrier to proving QMA=QMA$_1$ because it also shows that there is a “quantum” oracle such that QCMA is not equal to QCMA$_1$.
  - so, the result is the first nontrivial example that overcomes a “quantum” oracle separation.
Sketch of Proof

$L \in \text{QCMA}$

There is a p-time quantum algorithm $V$ such that:

- **(completeness)** If $x$ is in $L$, there is a bit-string $Y$ such that $V$ accepts with probability $p_x \geq 2/3$;
- **(soundness)** If $x$ is not in $L$, for any $Y$ the probability that $V$ accepts is $p_x \leq 1/3$.

- Wants to adjust it to a constant independent of $x$ with the help of the prover; then we can use the exact amplitude amplification [BHMT00] or the quantum rewinding [Wat09, KKMV09].
- The difficulty is:
  1. a malicious prover may send a cheating value so that soundness can fail;
  2. the original acceptance prob. $p_x$ may not be exactly expressible with polynomially many bits;
  3. the verifier may not be able to approximately adjust the acceptance prob. without error, even if he knows $p_x$ (due to the fact that the gate set is finite).
Sketch of Proof

- wants to adjust it to a constant independent of $x$ with the help of the prover; then we can use the exact amplitude amplification or the quantum rewinding.
- The difficulty is:
  1. a malicious prover may send a cheating value so that soundness can fail;
  2. the original acceptance prob. $p_x$ may not be exactly expressible with polynomially many bits;
  3. the verifier may not be able to approximately adjust the acceptance prob. without error, even if he knows $p_x$ (due to the fact that the gate set is finite).

Our Solution:
1. the verifier can catch the cheating since for the case $x \notin L$, the prover must give a “much different” value from the case $x \in L$ for a “large” adjusting;
2. we can assume that the circuit of the original verifier consists of Hadamard, Toffoli, and NOT gates, so assume $p_x = k/2^p(n)$ for some integer $k$;
3. we adjust the accepting probability “additively” (different from the “multiplicative” adjustments such as the exact amplitude amplification)
Our Protocol (Sketch)

Input $x$; bit string $w$ and integer $k$ from the prover

# $w$ is expected as the proof in the original system
# $k$ is expected such that $\frac{k}{2^{2p(n)}}$ equals the acceptance prob. $p_{x,w}$ on input $x$ and proof $w$ in the original system

1. REJECT if $k$ is too small relative to the value computed from the original completeness condition.

2. Do one of the two procedures with equal amplitude (by using the state $H\ket{0}$ as the conditional qubit):
   a. Simulate the original verifier;
   b. Generate a uniform superposition from 1 to $2^{2p(n)}$ and accept if this value is more than $k$

# When $x \in L$, the acceptance probability is exact $1/2$

3. Do the quantum rewinding [Wat09,KKMV09] by taking Step 2 as the base procedure.

step2(a):
$$p_{x,w} = \frac{1}{2} \frac{k}{2^{2p(n)}}$$

step2(b):
$$\frac{1}{2} \left( \frac{2^{p(n)} - k}{2^{p(n)}} \right)$$
Summary & Future Works

• Amplifying the completeness-soundness gap
  – 3SAT is in $\text{QMA}[2]_{\log}(1,1-1/n^{*}\log\text{poly}(n))$
  – How much can be the gap enhanced?
    • $\text{QMA}[2]_{\log}(1-1/n^2,1/n^2)=\text{BQP}$ [Bei09]

• Making two-sided error to one-sided error
  – QCMA=QCMA$_1$
  – QMA=QMA$_1$?
  – Is there another application for the additive adjustment of the success probability?
References
