NP **VS** QMA$_{\log}$(2)

SALMAN BEIGI

Institute for Quantum Information, California Institute of Technology
1200 E California Blvd, MC 305-16, Pasadena, California, 91125, USA

Although it is believed unlikely that NP-hard problems admit efficient quantum algorithms, it has been shown that a quantum verifier can solve NP-complete problems given a "short" quantum proof; more precisely, NP $\subseteq$ QMA$_{\log}$(2) where QMA$_{\log}$(2) denotes the class of quantum Merlin-Arthur games in which there are two unentangled provers who send two logarithmic size quantum witnesses to the verifier. The inclusion NP $\subseteq$ QMA$_{\log}$(2) has been proved by Blier and Tapp by stating a quantum Merlin-Arthur protocol for 3-coloring with perfect completeness and gap $\frac{1}{24n^6}$. Moreover, Aaronson *et al.* have shown the above inclusion with a constant gap by considering $\widetilde{O}(\sqrt{n})$ witnesses of logarithmic size. However, we still do not know if QMA$_{\log}$(2) with a constant gap contains NP. In this paper, we show that 3-SAT admits a QMA$_{\log}$(2) protocol with the gap $\frac{1}{n^{3+\epsilon}}$ for every constant $\epsilon > 0$.

1. Introduction

QMA is the class of problems that can be solved by a quantum polynomial time verifier (Arthur), given a polynomial size quantum proof by Merlin. The notion of quantum nondeterminism was first discussed by Knill [1], and then studied by Kitaev [2] and Watrous [3]. Later by the profound result of Kiteav *et al.* [4], who showed that the *local Hamiltonian problem* is QMA-complete, QMA was turned to an important complexity class. Although QMA and the local Hamiltonian problem are considered as the quantum analogue of NP and 3-SAT, respectively, there are other types of quantum Merlin-Arthur games without any classical analogue.

In the classical case, k Merlins, each one of which sends Arthur his own witness, is the same as one Merlin who sends all the messages together. However, in the quantum case we may consider the case where the k Merlins are not entangled and then send a separable state to Arthur. Thus, we cannot argue that one Merlin can send all the witnesses since he may cheat by sending an entangled state. So we obtain the non-trivial complexity class QMA(k) which has been first defined by Kobayashi *et al.* [5].

By definition, we have QMA = QMA(1) $\subseteq$ QMA(2) $\subseteq$ QMA(3) $\subseteq$ $\cdots$, so a question that arises is that whether we have equality somewhere or whether all the inclusions are strict. Also, the gap amplification problem is not an easy one for QMA(k). The first idea

toward proving gap amplification is to ask each Merlin to send polynomially many copies of his witness and then repeat the verification procedure many times. But this idea fails because one of the Merlins may cheat by entangling his copies. Then after the first round of the procedure we end up with some entanglement between different messages, which is not allowed. So there are two important questions regarding QMA(k): first, is there some k such that QMA$(k+1) = $ QMA(k), and second, can we amplify the gap in QMA(k) protocols? It is interesting that these two questions are related [5, 6, 7]; if we could amplify the error in QMA(k) protocols, then QMA$(2) = $ QMA(k), for any $k \geq 2$. Also, it has been proved by Aaronson *et al.* [7] that we can amplify the gap if the *Weak Additivity Conjecture* holds.

Other than changing the number of Merlins, we can consider the case where the size of the witnesses is less than poly(n). For instance, in the classical case $\log(n)$-size witnesses never help the verifier to solve any problem beyond P because he can check all such witnesses in polynomial time. But this argument fails in the quantum case and we can define the complexity classes QMA$_{\log}(k)$. Although the strong gap amplification protocol of [13] for QMA $=$ QMA(1) shows that for $k = 1$ we have QMA$_{\log}$ $=$ BQP, which is the same situation as in the classical case, we do not know any non-trivial upper bound for QMA$_{\log}(2)$.

Recently, Blier and Tapp [8] have shown that QMA$_{\log}(2)$ with perfect completeness and soundness $1 - \frac{1}{24n^6}$ contains the 3-coloring problem, turning this complexity class to an interesting one which contains both BQP and NP. The only issue regarding this result is that the gap should be small ($\frac{1}{24n^6}$). In contrast, Aaronson *et al.* [7] have proved that NP has a constant gap quantum Merlin-Arthur protocol in which there are $\widetilde{O}(\sqrt{n})$ Merlins each one of which sends a $\log(n)$-qubit state.

In this paper, we show that 3-SAT is in QMA$_{\log}(2)$ with the gap $\frac{1}{n^{3+\epsilon}}$ for any constant $\epsilon > 0$. Comparing to [8], we improve the gap at the cost of losing perfect completeness.

1.1. *Main idea*

Suppose that Arthur is given a quantum state over two registers of size $\log(n)$, and wants to recognize whether this state is entangled or not. We do not know any algorithm to recognize entanglement, but if two unentangled Merlins give Arthur two witnesses, by comparing them to his state he can check whether the state is separable or not. It means that a two-prover Merlin-Arthur protocol can recognize separable states. On the other hand, Gurvits [9] has shown that given the classical description of a quantum state over two registers, it is NP-complete to decide whether the state is separable or not. Therefore, we have a way of comparing QMA$_{\log}(2)$ and NP. This is the main idea behind our result, but it should be slightly changed in order to obtain a larger gap.

2. Definitions and basic properties

Through this paper we assume the basic knowledge on theory of quantum computing [10] and complexity theory [11, 12].

2.1. QMA$_{\log}$(2)

Definition 1 *Let k be an integer, and $a = a(n), b = b(n)$ be functions such that, $0 \leq b < a \leq 1$. Also, let $f(n)$ be a function of n. Then the complexity class* QMA$_{f(n)}(k, a, b)$ *consists*

of languages L for which there exists a quantum polynomial time verifier V such that for any $x \in \{0,1\}^n$,

- *Completeness: if* $x \in L$, *then there are* $O(f(n))$-*qubit states* $|\psi_1\rangle, \ldots, |\psi_k\rangle$ *such that* $\Pr\left[V \text{ accepts } |x\rangle|\psi_1\rangle \ldots |\psi_k\rangle\right] \geq a.$

- *Soundness: if* $x \notin L$, *then for any* $O(f(n))$-*qubit states* $|\psi_1\rangle, \ldots, |\psi_k\rangle$ *we have* $\Pr\left[V \text{ accepts } |x\rangle|\psi_1\rangle \ldots |\psi_k\rangle\right] \leq b.$

Here, by convention when the number k or function $f(n)$ are not mentioned we mean that $k = 1$ and $f(n)$ is a polynomial of n. Also, we let $\mathsf{QMA}_{f(n)}(k)$ to be

$$\mathsf{QMA}_{f(n)}(k) = \bigcup_{a(n),b(n)} \mathsf{QMA}_{f(n)}(k,a,b), \tag{1}$$

where the union is taken over all functions $a(n)$ and $b(n)$ such that $0 \leq b(n) < a(n) \leq 1$, and $a(n) - b(n) > n^{-c}$ holds for sufficiently large n and some constant c.

Other than the usual case $f(n) = \text{poly}(n)$, $f(n) = \log(n)$ is also of interest. Marriott and Watrous [13] have considered $f(n) = \log(n)$ for the first time.

Theorem 1 [13] $\mathsf{QMA}_{\log} = \mathsf{BQP}$.

Proof of this theorem is based on a gap amplification argument without increasing the size of witness, which is not known for $\mathsf{QMA}(2)$. So we cannot argue that $\mathsf{QMA}_{\log}(2)$ is the same as BQP. Indeed, it is a non-trivial complexity class due to the result of Blier and Tapp.

Theorem 2 [8] 3-coloring *belongs to* $\mathsf{QMA}_{\log}(2, 1, 1 - \frac{1}{24n^6})$.

2.2. *2-out-of-4-SAT*

To prove the containment $\mathsf{NP} \subseteq \mathsf{QMA}_{\log}(2)$ we should find a protocol to solve some NP-complete problem in $\mathsf{QMA}_{\log}(2)$. Although the most well-known such problem is 3-SAT, it is convenient for us to use a variant of this problem called 2-out-of-4-SAT.

Any instance of 2-out-of-4-SAT consists of some clauses each of which contains exactly four literals, and is satisfied if in each clause exactly two of the literals are true. 2-out-of-4-SAT can also be expressed as follows.

The clauses of the problem are vectors $|a_1\rangle, |a_2\rangle, \ldots, |a_m\rangle$ of the form

$$|a_k\rangle = \sum_{j=1}^{n} c_{kj} |j\rangle, \tag{2}$$

where $c_{kj} = 0$ or $\pm\frac{1}{2}$, and for each k there are exactly four non-zero c_{kj}, $1 \leq j \leq n$. We say that the j-th variable appears in clause $|a_k\rangle$ if c_{kj} is non-zero. Now the problem is to decide whether there exists a vector $|\psi\rangle$ orthogonal to all $|a_k\rangle$'s and of the form

$$|\psi\rangle = \sum_{j=1}^{n} \pm\frac{1}{\sqrt{n}} |j\rangle. \tag{3}$$

Lemma 1 [7] *There exists a polynomial time Karp reduction that maps a* 3-SAT *instance* α *to a* 2-out-of-4-SAT *instance* β *such that*

- *If* α *has* n *variables and* $n' \geq n$ *clauses, then* β *has* $O(n'\mathrm{poly}\log(n'))$ *variables and* $O(n'\mathrm{poly}\log(n'))$ *clauses.*

- *Every variable of* β *occurs in at most* c *clauses, for some constant* c.

- *The reduction is a PCP, meaning that satisfiable instances map to satisfiable instances, while unsatisfiable instances map to instances in which at most a constant fraction of the clauses can be satisfied at the same time.*

3. Complexity of recognizing entanglement

Let H be a hermitian matrix of polynomial size (over $\log(n)$ qubits). Then, the problem of maximizing $\langle\phi|H|\phi\rangle$ over all states $|\phi\rangle$ is an eigenvalue problem and can be solved efficiently. Now assume that we restrict $|\phi\rangle$ to be a separable state. (Here we assume that H acts over two registers.) Then the above maximization is an NP-hard problem due to the following observation by Gurvits [9].

Let H be of the form

$$H = \begin{pmatrix} 0 & B_1 & \cdots & B_s \\ B_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ B_s & 0 & \ldots & 0 \end{pmatrix}, \tag{4}$$

where B_j, $1 \leq j \leq s$, is a hermitian matrix. Observe that

$$\langle\psi|\langle\phi|H|\phi\rangle|\psi\rangle = \langle\phi|H(|\psi\rangle)|\phi\rangle,$$

where

$$H(|\psi\rangle) = \begin{pmatrix} 0 & \langle\psi|B_1|\psi\rangle & \cdots & \langle\psi|B_s|\psi\rangle \\ \langle\psi|B_1|\psi\rangle & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \langle\psi|B_s|\psi\rangle & 0 & \ldots & 0 \end{pmatrix}. \tag{5}$$

This means that the maximum of $\langle\psi|\langle\phi|H|\phi\rangle|\psi\rangle$, for a fixed $|\psi\rangle$, is equal to the maximum eigenvalue of $H(|\psi\rangle)$. $H(|\psi\rangle)$ is a rank-two matrix and its eigenvalues can be simply computed. Hence,

$$\max_{|\phi\rangle|\psi\rangle} \langle\psi|\langle\phi|H|\phi\rangle|\psi\rangle = \max_{|\psi\rangle} \left[\langle\psi|B_1|\psi\rangle^2 + \cdots + \langle\psi|B_s|\psi\rangle^2 \right]^{1/2}. \tag{6}$$

Gurvits [9] has referred to [14] (which states that estimating the right hand side of Eq. (6) is NP-hard) and concluded the NP-hardness of computing the left hand side of Eq. (6).

In this paper, we take the advantage of Eq. (6) in another direction. Suppose two (unentangled) quantum provers send the state $|\phi\rangle|\psi\rangle$ to a quantum polynomial time verifier. Then the verifier can estimate $\langle\psi|\langle\phi|H|\phi\rangle|\psi\rangle$ (using the idea of [4, 15]) or equivalently the

right hand side of Eq. (6). Thus, we conclude that $\mathsf{QMA}_{\log}(2)$ contains NP. Here we slightly change this idea in order to obtain a larger gap in the $\mathsf{QMA}_{\log}(2)$ protocol.

4. $\mathsf{NP} \subseteq \mathsf{QMA}_{\log}(2)$

In this section we prove our main result.

Theorem 3 *For every constant $\epsilon > 0$, 3-SAT is in $\mathsf{QMA}_{\log}(2, a, a - \frac{1}{n^{3+\epsilon}})$ for some a independent of ϵ.*

To prove this theorem we give a Merlin-Arthur protocol for the 2-out-of-4-SAT problem. This protocol consists of two parts: first, given a satisfying assignment we should check whether it is a *proper state*, i.e., a state of the form of Eq. (3); second, we should check whether it is orthogonal to all vectors in the 2-out-of-4-SAT instance. We state each one of these parts in a separate lemma.

Lemma 2 *Let $\epsilon > 0$ be a constant. Then there exists a Merlin-Arthur protocol in which Arthur upon receiving the state $|\phi\rangle|\psi\rangle$ can check whether $|\psi\rangle$ is $(5n^{-\epsilon/4})$-close, in trace distance, to a proper state or not. More precisely, if $|\psi\rangle$ is proper (and $|\phi\rangle$ is chosen correctly), then Arthur accepts with probability*

$$\frac{1}{2} + \frac{1}{3n}\left(2 - \frac{2}{n}\right)^{1/2}, \tag{7}$$

and if it is not $(5n^{-\epsilon/4})$-close to a proper state, then he accepts with probability at most

$$\frac{1}{2} + \frac{1}{3n}\left(2 - \frac{2}{n}\right)^{1/2} - \frac{1}{20n^{3+\epsilon}}. \tag{8}$$

Note that the acceptance probability of this protocol is never more than Eq. (7).

Now consider an instance α of 3-SAT. Arthur can reduce α to an instance β of 2-out-of-4-SAT with the conditions in Lemma 1, and ask Merlin to send him a satisfying assignment of β. Then if β is satisfiable, Arthur by measuring Merlin's state can verify whether it is orthogonal to $|a_k\rangle$'s or not. This idea is elaborated by Aaronson *et al.* [7] to give a protocol for checking whether a given proper state is a satisfying assignment for β or not.

Lemma 3 [7] *Let us assume that Merlin is restricted to send a proper state. Then Arthur can solve 3-SAT with perfect completeness and constant soundness.*

The following corollary is a straightforward consequence of this lemma.

Corollary 1 [7] *Let us assume that Merlin is restricted to send a state that is δ-close, in trace distance, to a proper state for a constant $\delta > 0$. Then Arthur can solve 3-SAT with perfect completeness and constant soundness.*

Now we prove Theorem 3 assuming Lemma 2.

Proof of Theorem 3: Given a 3-SAT instance α of size n (for a sufficiently large n), Arthur reduces it to a 2-out-of-4-SAT instance β over m variables according to Lemma 1, and asks Merlins to send him $|\phi\rangle|\psi\rangle$ where $|\psi\rangle$ is (a proper state and) a satisfying assignment for β. Then he applies one of the tests in Lemmas 2 or 3, each with probability $1/2$.

If α is satisfiable, then Arthur accepts with probability

$$a = \frac{1}{2} + \frac{1}{2}\left[\frac{1}{2} + \frac{1}{3m}\left(2 - \frac{2}{m}\right)^{1/2}\right]. \tag{9}$$

If it is not satisfiable, then there are two cases. If $|\psi\rangle$ is not $(5m^{-\epsilon'/4})$-close to a proper state, then Arthur accepts with probability at most

$$b_1 = \frac{1}{2} + \frac{1}{2}\left[\frac{1}{2} + \frac{1}{3m}\left(2 - \frac{2}{m}\right)^{1/2} - \frac{1}{20m^{3+\epsilon'}}\right]. \tag{10}$$

Also, if $|\psi\rangle$ is $(5m^{-\epsilon'/4})$-close (and then 2^{-10}-close) to a proper state (which is not a satisfying assignment), then he accepts with probability at most

$$b_2 = \frac{1}{2}s + \frac{1}{2}\left[\frac{1}{2} + \frac{1}{3m}\left(2 - \frac{2}{m}\right)^{1/2}\right], \tag{11}$$

where the constant s denotes the soundness of the test of Corollary 1 corresponding to $\delta = 2^{-10}$. Here we use the fact that the maximum acceptance probability of the protocol of Lemma 2 is given by Eq. (7).

Now observe that $b_2 < b_1$ for sufficiently large m. Therefore, 3-SAT is in QMA$_{\log}(2, a, b)$, where

$$b = \frac{1}{2} + \frac{1}{2}\left[\frac{1}{2} + \frac{1}{3m}\left(2 - \frac{2}{m}\right)^{1/2}\right] - \frac{1}{n^{3+\epsilon}} = a - \frac{1}{n^{3+\epsilon}}. \tag{12}$$

Here we replace ϵ' with ϵ to consider the poly-logarithmic blowup in the size of problem by reducing it from a 3-SAT instance to a 2-out-of-4-SAT instance, and to eliminate the constants appeared in Lemma 2. $\square$

So the only remaining part is the proof of Lemma 2.

4.1. *Proof of Lemma 2*

Consider a Hilbert space with the orthonormal basis $\{|1\rangle, \ldots, |n\rangle\}$. For any $1 \le j < l \le n$ define the hermitian matrix

$$B_{jl} = |j\rangle\langle l| + |l\rangle\langle j|,$$

and let

$$
H = \begin{pmatrix} 0 & B_{1,2} & \cdots & B_{(n-1)n} \\ B_{1,2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ B_{(n-1)n} & 0 & \cdots & 0 \end{pmatrix},
\tag{13}
$$

where all B_{jl}, $1 \le j < l \le n$, appear as a submatrix of H.

We show that the maximum of $\langle\psi|\langle\phi|H|\phi\rangle|\psi\rangle$ over all states $|\psi\rangle$ and $|\phi\rangle$ occurs when $|\psi\rangle$ is a proper state. In this case, given the state $|\phi\rangle|\psi\rangle$ one can estimate $\langle\psi|\langle\phi|H|\phi\rangle|\psi\rangle$ in order to check whether $|\psi\rangle$ is a proper state or not. However, H is not a measurement operator and it is not clear how we can estimate $\langle\psi|\langle\phi|H|\phi\rangle|\psi\rangle$. So we need some modifications.

It is easy to see that $\lambda \ne 0$ is an eigenvalue of H iff λ^2 is an eigenvalue of $\sum_{j,l} B_{jl}^2$. Then, $\|H\|_\infty$, the infinite-norm[a] of matrix H, satisfies

$$
\|H\|_\infty^2 = \|\sum_{j,l} B_{jl}^2\|_\infty \le \sum_{j,l} \|B_{jl}\|_\infty^2 = \binom{n}{2} \le n^2.
$$

Therefore, $\frac{1}{2}I + \frac{1}{3n}H$ is a positive semi-definite matrix (and in fact an $O(\log(n))$-local Hamiltonian) with norm $\|\frac{1}{2}I + \frac{1}{3n}H\|_\infty < 1$. Thus, by the techniques presented in [4, 15], having the state $|\phi\rangle|\psi\rangle$ Arthur can throw a coin with probability of head being

$$
\langle\psi|\langle\phi|\left(\frac{1}{2}I + \frac{1}{3n}H\right)|\phi\rangle|\psi\rangle,
\tag{14}
$$

and accept if it is head. Hence, by Eq. (6), if $|\phi\rangle$ is the right state, the probability of acceptance is equal to

$$
\frac{1}{2} + \frac{1}{3n} \max_{|\psi\rangle} \left[\sum_{j,l} \langle\psi|B_{jl}|\psi\rangle^2 \right]^{1/2}.
\tag{15}
$$

Now we need the following lemma.

Lemma 4 $\sum_{j,l}\langle\psi|B_{jl}|\psi\rangle^2 \le 2 - \frac{2}{n}$, *and equality holds iff* $|\psi\rangle$ *is a proper state. Also, for sufficiently large n if*

$$
\sum_{j,l}\langle\psi|B_{jl}|\psi\rangle^2 \ge 2 - \frac{2}{n} - \frac{1}{n^{2+\epsilon}},
\tag{16}
$$

then $|\psi\rangle$ *is* $(5n^{-\epsilon/4})$-*close to a proper state in trace distance.*

Using this lemma, if $|\psi\rangle$ is a proper state, the probability of acceptance is equal to

$$
\frac{1}{2} + \frac{1}{3n}\left(2 - \frac{2}{n}\right)^{1/2},
\tag{17}
$$

and if it is greater than

$$
\frac{1}{2} + \frac{1}{3n}\left(2 - \frac{2}{n}\right)^{1/2} - \frac{1}{20n^{3+\epsilon}},
\tag{18}
$$

---

[a] $\|X\|_\infty$ denotes the maximum eigenvalue of $|X| = \sqrt{XX^\dagger}$.

then $|\psi\rangle$ is $(5n^{-\epsilon/4})$-close to a proper state. □

So it remains to prove Lemma 4.

Proof of Lemma 4: Let

$$|\psi\rangle = \sum_{j=1}^{n} x_j \, |j\rangle \tag{19}$$

be a normalized state. Then

$$
\begin{aligned}
\sum_{j,l} \langle\psi|B_{jl}|\psi\rangle^2 &= \sum_{j<l} (\overline{x}_j x_l + x_j \overline{x}_l)^2 \\
&= \sum_{j<l} \left(\overline{x}_j^2 x_l^2 + x_j^2 \overline{x}_l^2 + 2|x_j|^2 |x_l|^2 \right) \\
&= \left(\sum_j \overline{x}_j^2 \right)\left(\sum_j x_j^2 \right) - \sum_j |x_j|^4 + 2\sum_{j<l} |x_j|^2 |x_l|^2 \\
&= |\sum_j x_j^2|^2 + \left(\sum_j |x_j|^2 \right)^2 - 2\sum_j |x_j|^4,
\end{aligned}
\tag{20}
$$

where $\overline{x}$ denotes the complex conjugate of the number x.

Using equation $\sum_{j=1}^{n} |x_j|^2 = 1$ we obtain the inequalities

$$\sum_j |x_j|^4 \geq \frac{1}{n} \tag{21}$$

and

$$|\sum_j x_j^2|^2 \leq 1. \tag{22}$$

Hence, combining with Eq. (20) we find that $\sum_{j,l} \langle\psi|B_{jl}|\psi\rangle^2 \leq 2 - \frac{2}{n}$, and equality holds iff both Eqs. (21) and (22) are equalities, i.e., for any $1 \leq j \leq n$

$$x_j^2 = \frac{1}{n} \, e^{i\theta}, \tag{23}$$

for a constant θ, or equivalently iff $|\psi\rangle$ is a proper state.

Now assume that Eq. (16) holds; we show that $|\psi\rangle$ is close to a proper state. By Eq. (20) we have

$$\sum_{j,l}\langle\psi|B_{jl}|\psi\rangle^2 = |\sum_j x_j^2|^2 + \left(\sum_j |x_j|^2 \right)^2 - 2\sum_j |x_j|^4 \geq 2 - \frac{2}{n} - \frac{1}{n^{2+\epsilon}}. \tag{24}$$

So comparing to Eqs. (21) and (22) we find that

$$\sum_j |x_j|^4 \leq \frac{1}{n} + \frac{1}{n^{2+\epsilon}}, \tag{25}$$

and

$$|\sum_j x_j^2|^2 \geq 1 - \frac{1}{n^{2+\epsilon}}. \tag{26}$$

Observe that

$$\sum_j \left(|x_j|^2 - \frac{1}{n}\right)^2 = \sum_j \left(|x_j|^4 + \frac{1}{n^2} - \frac{2}{n}|x_j|^2\right) = \sum_j |x_j|^4 - \frac{1}{n}. \tag{27}$$

Therefore, by Eq. (25) for every j

$$|\,|x_j|^2 - \frac{1}{n}\,| \leq \frac{1}{n^{1+\delta}}, \tag{28}$$

where $\delta = \epsilon/2$, and then

$$|\,|x_j| - \frac{1}{\sqrt{n}}\,| \leq \frac{\sqrt{n}}{n^{1+\delta}}. \tag{29}$$

Also, using Eq. (26) we have

$$\left(\sum_j |x_j|^2\right)^2 - |\sum_j x_j^2|^2 \leq \frac{1}{n^{2+\epsilon}}, \tag{30}$$

and since

$$\left(\sum_j |x_j|^2\right)^2 - |\sum_j x_j^2|^2 = 2\sum_{j<l}(|x_j x_l|^2 - \mathrm{Re}\, x_j^2 \bar{x}_l^2), \tag{31}$$

and $|x_j x_l|^2 - \mathrm{Re}\, x_j^2 \bar{x}_l^2$ is always non-negative we obtain

$$|x_j x_l|^2 - \mathrm{Re}\, x_j^2 \bar{x}_l^2 \leq \frac{1}{n^{2+\epsilon}}, \tag{32}$$

for every j and l.

Now let $x_j = s_j r_j e^{i\theta_j}$, where $s_j \in \{+1, -1\}$, r_j is a non-negative real number, and $-\frac{\pi}{2} < \theta_j \leq \frac{\pi}{2}$. Then Eq. (29) is equivalent to

$$|r_j - \frac{1}{\sqrt{n}}\,| \leq \frac{\sqrt{n}}{n^{1+\delta}}. \tag{33}$$

Also, by Eqs. (28) and (32)

$$1 - \mathrm{Re}\, e^{2i(\theta_j - \theta_l)} \leq \frac{1}{n^{2+\epsilon}}\left(\frac{1}{n} - \frac{1}{n^{1+\delta}}\right)^{-2} = (n^\delta - 1)^{-2} \leq \frac{2}{n^\epsilon}, \tag{34}$$

for sufficiently large n. Without loss of generality, we assume that $\theta_1 = 0$; thus for every j we have

$$1 - \mathrm{Re}\, e^{2i\theta_j} \leq \frac{2}{n^\epsilon}, \tag{35}$$

and since $-\frac{\pi}{2} < \theta_j \leq \frac{\pi}{2}$,

$$1 - \mathrm{Re}\, e^{i\theta_j} \leq \frac{2}{n^\epsilon}. \tag{36}$$

Now using $(\mathrm{Re}\, e^{i\theta_j})^2 + (\mathrm{Im}\, e^{i\theta_j})^2 = 1$, it is easy to see that

$$|1 - e^{i\theta_j}| \leq \frac{2}{n^\delta}. \tag{37}$$

Therefore, by Eqs. (33) and (37)

$$
\begin{aligned}
|\, r_j e^{i\theta_j} - \frac{1}{\sqrt{n}}\,| &\leq |r_j - \frac{1}{\sqrt{n}}| + |r_i(1 - e^{i\theta_j})| \\
&\leq \frac{\sqrt{n}}{n^{1+\delta}} + \left(\frac{1}{\sqrt{n}} + \frac{\sqrt{n}}{n^{1+\delta}}\right)\frac{2}{n^\delta},
\end{aligned}
\tag{38}
$$

and then

$$|\, r_j e^{i\theta_j} - \frac{1}{\sqrt{n}}\,| \leq \frac{10\sqrt{n}}{n^{1+\delta}}. \tag{39}$$

Now define the proper state

$$|\psi'\rangle = \sum_j \frac{s_j}{\sqrt{n}} |j\rangle. \tag{40}$$

We have

$$
\begin{aligned}
|\langle\psi'|\psi\rangle| &= |\sum_j \frac{1}{\sqrt{n}} s_j^2 r_j e^{i\theta_j}| \\
&= \frac{1}{\sqrt{n}}|\sum_j r_j e^{i\theta_j}| \\
&\geq \frac{1}{\sqrt{n}}\left(\sqrt{n} - |\sum_j \left(r_j e^{i\theta_j} - \frac{1}{\sqrt{n}}\right)|\right) \\
&\geq 1 - \frac{1}{\sqrt{n}}\sum_j |r_j e^{i\theta_j} - \frac{1}{\sqrt{n}}|.
\end{aligned}
\tag{41}
$$

Using Eq. (39) we obtain

$$|\langle\psi'|\psi\rangle| \geq 1 - \sqrt{n}\,\frac{10\sqrt{n}}{n^{1+\delta}} = 1 - \frac{10}{n^\delta}. \tag{42}$$

Therefore,

$$\|\,|\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'|\,\|_{\mathrm{tr}} = \left(1 - |\langle\psi'|\psi\rangle|^2\right)^{1/2} \leq \left(\frac{20}{n^\delta}\right)^{1/2} < 5n^{-\delta/2}. \tag{43}$$

We are done. $\square$

5. Conclusion

Although the gap in our QMA$_{\log}$(2) protocol for 3-SAT is larger than the gap in the proof of Blier and Tapp ($\frac{1}{n^{3+\epsilon}}$ versus $\frac{1}{24n^6}$), their protocol is one-sided error. So one direction to improve this result is to turn it into a protocol with perfect completeness.

Another open question is that whether the optimal gap depends on n, or whether there exists a constant gap QMA$_{\log}$(2) protocol for NP. This question is related to the problem of

whether recognizing states that are δ-close to a separable state, for some *constant $\delta > 0$*, is NP-hard or not.

Acknowledgements

References

1. E. Knill, *Quantum randomness and nondeterminism*, Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996, quantph/9610012.
2. A. Kitaev, *Quantum NP*, AQIP99: Second Workshop on Algorithms in Quantum Information Processing, 1999.
3. J. Watrous, *Succinct quantum proofs for properties of finite groups*, Proceedings of IEEE FOCS'2000, pp. 537-546, 2000.
4. A. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, American Mathematical Society, 2002.
5. H. Kobayashi, K. Matsumoto, and T. Yamakami, *Quantum Certificate Verification: Single versus Multiple Quantum Certificates*, quant-ph/0110006.
6. H. Kobayashi, K. Matsumoto, and T. Yamakami, *Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?*, Lecture Notes in Computer Science, 2003, vol. 2906, pp. 189-198.
7. S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor, *The Power of Unentanglement*, Theory of Computing, 5 (2009) pp. 1-42.
8. Hugue Blier and Alain Tapp, *All languages in NP have very short quantum proofs*, Proceedings of the ICQNM, 2009, 34-37.
9. Leonid Gurvits, *Classical complexity and quantum entanglement*, Journal of Computer and System Sciences, 69 (2004) 448-484.
10. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
11. Michael Sipser, *Introduction to the Theory of Computation*, PWS Publishing Company, 2005.
12. C. H, Papadimitriou, *Computational Complexity*, Addison-Wesley Publishing Company, Inc., 1994.
13. Chris Marriott and John Watrous, *Quantum Arthur-Merlin Games*, Computational Complexity, 14(2): 122-152, 2005.
14. A. Ben-Tal and A. Nemirovski, *Robust convex optimization*, Mathematics of Operational Research, Vol. 23, 4 (1998), 769-805.
15. Dorit Aharonov and Tomer Naveh, *Quantum NP - A Survey*, quant-ph/0210077.