BQP $\neq$ QMA

Ping Wang and Yiting Su

Shenzhen University, Shenzhen 518060, China
wangping@szu.edu.cn, suyiting2020@email.szu.edu.cn

Abstract. The relationship between complexity classes BQP and QMA is analogous to the relationship between P and NP. In this paper, we design a quantum bit commitment problem that is in QMA, but not in BQP. Therefore, it is proved that BQP $\neq$ QMA. That is, problems that are verifiable in quantum polynomial time are not necessarily solvable in quantum polynomial time, the quantum analog of P $\neq$ NP.

Keywords: BQP, QMA, complexity theory, quantum complexity theory

1 Introduction

Quantum complexity theory is a branch of computational complexity theory concerned with the definition of complexity classes using quantum computers, a computational model based on quantum mechanics. BQP and QMA are two important quantum complexity classes [1,2].

Definition 1 (Bounded-error Quantum Polynomial Time (BQP)). *A language $L \in BQP$ if and only if there exists a $poly(|x|)$ time quantum algorithm f, such that:*

- $\forall x \in L,\ Pr(f(x) = 1) \geq 2/3.$
- $\forall x \notin L,\ Pr(f(x) = 1) \leq 1/3.$

Definition 2 (Quantum Merlin Arthur (QMA)). *Let $\mathcal{B}$ denote the Hilbert space of one qubit. A language $L \in QMA$ if and only if there exists a $poly(|x|)$ time quantum verifier V, such that:*

- $\forall x \in L,\ \exists|\psi\rangle \in \mathcal{B}^{poly(|x|)},\ Pr(V(x, |\psi\rangle) = 1) \geq 2/3.$
- $\forall x \notin L,\ \forall|\psi\rangle \in \mathcal{B}^{poly(|x|)},\ Pr(V(x, |\psi\rangle) = 1) \leq 1/3.$

The no-communication theorem (or no-signaling principle) [3,4,5] shows that communication between two observers is not possible using entanglement alone. In fact, if two observers could transfer information simply by entanglement without additional information exchange, this would lead to the paradox of faster-than-light (FTL) communication. We have the following theorem and corollary.

Theorem 1 (No-communication Theorem). *It is impossible for one observer to communicate information to another observer during the measurement of an entangled quantum state by making a measurement of a subsystem of the total state.*

Corollary 1. *Suppose that Alice and Bob share a Bell state (a, b), where a denotes one qubit of the Bell state and b denotes the other one. Alice keeps a and Bob keeps b, respectively. Without further information exchange, there is no way for Bob to determine afterward whether a has been measured or not.*

The quantum bit commitment problem (or game) proposed in the following section essentially relies on the no-communication theorem and corollary 1.

2 The Quantum Bit Commitment Problem

Bit commitment is a cryptographic primitive that allows Alice to commit to a chosen value (e.g., a bit) while keeping it hidden from Bob in the commit phase; Alice cannot change the value after she has committed to it and can reveal the committed value with certain proof in the opening phase. Without loss of generality, we focus on the verifier-based definition of the decision problem of the quantum bit commitment in an error-free environment for simplicity. Unless otherwise stated, "randomly" in the following usually means randomly with equal probability.

The basic idea of the proposed QBC problem is that: Alice and Bob share n Bell states. Alice has two choices (representing the commitments $x = 1$ and $x = 0$, respectively): either to measure some qubits on her hand at random, or not to measure any qubits at all. Alice then provides evidence R to finish the commit phase. The key to the design is that, on the one hand, Alice cannot change her commitment due to R, i.e., if Alice chooses to measure certain qubits, then in the opening phase, she cannot convince Bob that she did not measure any qubits as the measurement is not reversible; if Alice chooses not to measure any qubits, then in the opening phase, she cannot convince Bob that she has measured certain qubits as R is bound to the measurement result and the measurement result is unpredictable. On the other hand, Bob should not be able to distinguish Alice's commitment based on R before the opening phase. That is, R should be the hidden value of the measurement result, rather than the direct measurement result. In detail, we have the following definition.

Definition 3 (Quantum Bit Commitment (Decision Problem)). *Let n and m be integers, such that n is divisible by $2m$, denoted as $n = ml$ (e.g., $m = 64$, $l = 16$ and $n = 1024$). Assume that Alice and Bob share n Bell states, which are denoted as $(a_i, b_i) \triangleq \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ with $1 \leq i \leq n$, where a_i represents one qubit of the ith Bell state and b_i represents the other one. Let $A \triangleq (a_1, a_2, ..., a_n)$ and $B \triangleq (b_1, b_2, ..., b_n)$. Alice keeps the qubit sequence A and Bob keeps B.*

If Alice wants to commit to $x = 0$, she generates an m-bit random bit string $R \triangleq r_1 r_2 ... r_m$, where each bit r_i has a probability of $1/2$ of being 0 and a probability of $1/2$ of being 1.

If Alice wants to commit to $x = 1$, she randomly selects m qubits from A, denoted in the order as $(a_{j_1}, a_{j_2}, \ldots, a_{j_m})$, such that the distance ($d_i = j_{i+1} - j_i$) of any two adjacent selected qubits satisfies: $\frac{l}{2} \leq d_i < \frac{3l}{2}$ for all $1 \leq i < m$.

For each selected qubit a_{j_i} $(1 \leq i \leq m)$, Alice randomly chooses the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$ to measure it (i.e., each qubit corresponds to a randomly selected basis), and records the measurement basis and the measurement result y_i (i.e., if the measurement result of a_{j_i} is $|0\rangle$ or $|+\rangle$, it is recorded as $y_i = 0$; if the measurement result of a_{j_i} is $|1\rangle$ or $|-\rangle$, it is recorded as $y_i = 1$). For each selected qubit a_{j_i} $(1 \leq i \leq m)$, Alice generates an output bit by $r_i = (y_i + y_{i+1} + d_i)$ mod 2, where $y_{m+1} \triangleq y_1$ and $d_m \triangleq n - j_m + j_1$. Then, Alice set $R \triangleq r_1 r_2 ... r_m$.

Finally, Alice announces R as evidence of commitment. The problem is, given $x' = 0$ or 1, determine whether x' is Alice's commitment.

Note that the above QBC problem can be easily extended to the problem of committing a k-bit x. In such case, Alice and Bob should share nk Bell states. The decision problem is to determine whether a given k-bit instance x' is a Yes-instance or a No-instance (Only one Yes-instance exists, i.e., $x' = x$; all other $2^k - 1$ instances are No-instances). The computational problem is to find the unique solution x.

For the quantum bit commitment decision problem p defined by Definition 3, we will show that the verifier Bob can not figure out the value x according to the publicly available information. Hence, $p \notin$ BQP. Furthermore, for any instance x', the prover Alice can convince Bob it is a Yes-instance or a No-instance with the proof. Therefore, $p \in$ QMA.

In fact, in the subsequent opening phase, Alice reveals her commitment x with corresponding proofs. For the case $x = 0$, Alice sends A (as the proof) to Bob. For each $a_i \in A$, $b_i \in B$ with $1 \leq i \leq n$, Bob performs Bell state verification on (a_i, b_i). If any verification fails, Bob detects that Alice is cheating and terminates the game. Bob accepts the commitment $x = 0$ if and only if all verifications pass.

For the case $x = 1$, Alice announces the indexes of all the measured qubits $(j_1, j_2, \ldots, j_m)$, the measurement results $(y_1, y_2, \ldots, y_m)$, and the corresponding measurement bases. Alice sends all unmeasured qubits in A (denoted as $\tilde{A}$) to Bob. To verify Alice's commitment $x = 1$, Bob measures each qubit in $(b_{j_1}, b_{j_2}, ..., b_{j_m})$ from B with the corresponding basis provided by Alice, such that a_{j_i} and b_{j_i} were measured using the same basis. Let $(y'_1, y'_2, ..., y'_m)$ denote the corresponding measurement results of $(b_{j_1}, b_{j_2}, ..., b_{j_m})$. Then Bob performs the following checks: 1) Bob checks whether all the equations $y'_i = y_i$ $(1 \leq i \leq m)$ hold, i.e., the two qubits in each pair (a_{j_i}, b_{j_i}) measured with the same basis should have the same result. 2) For each measured qubit, Bob checks whether all equations $r_i = (y_i + y_{i+1} + d_i)$ mod 2 hold for $1 \leq i \leq m$. 3) Bob checks whether all the equations $\frac{l}{2} \leq d_i < \frac{3l}{2}$ hold for $1 \leq i < m$. 4) For each $a_i \in \tilde{A}$ with $b_i \in B$, Bob performs Bell state verification on (a_i, b_i). If any check fails, Bob detects that Alice is cheating and terminates the game. Bob accepts the commitment $x = 1$ if and only if all checks pass.

2.1 $p \notin$ BQP

In this section, we will show that if Alice behaves as described in the QBC game, Bob cannot figure out x through the qubit sequence B and the bit string R.

On the one hand, according to the no-communication theorem, Bob learns nothing about Alice's operations (measurements) by entanglement. For any qubit in A (and the same in B), Bob cannot tell if the qubit has been measured (or if it has collapsed). Therefore, Bob gets no information about x based on the qubit sequence B alone.

On the other hand, for each qubit a_{j_i} with $1 \leq i \leq m$, Alice randomly (with equal probability) chooses either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$ to perform the measurement. Then, based on the superposition principle and the entanglement property (i.e., $(a_i, b_i) = \frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{|++\rangle+|--\rangle}{\sqrt{2}}$), the measurement leads to a collapse of the quantum state. The probability of getting a result of 0 is 1/2 and the probability of getting a result of 1 is 1/2, a result that neither Alice nor Bob could predict. For the case of $x = 1$, it means that the output $R \triangleq r_1 r_2 ... r_m$ based on the measurement results can be any binary string $R \in \{0,1\}^m$. That is, R and a random number of m bits are indistinguishable. Therefore, Bob cannot distinguish between two commitments based on the m output bits R alone.

Furthermore, if Alice chooses to measure certain qubits (i.e., $x = 1$), then based on the Bell state entanglement property, Bob has exactly the same set of qubits B as A. In the following, we will show that Bob cannot figure out x through the qubit sequence B and the m output bits R. In fact, if R is a completely random binary string for Bob, then Bob gets no information about Alice's choice x. Moreover, since the positions of the measured qubits are unknown to Bob, it is impossible to divide the whole sequence of qubits B into multiple samples, but only to analyze the quantum sequence B by looking at it as a whole (one sample), thus avoiding distinguishing the commitments with statistical methods by POVM measurements.

For any instance $R \triangleq r_1 r_2 ... r_m$ with $x = 1$, there are many possible states that can output the same R. For example, there are two states that have different measurement bases but yield the same measurement outcome, or two states that have different positions for the i-th measured qubit but have the same parity of the index, and both states will output the same R. Therefore, based on the no-communication theorem, Bob cannot infer which qubit was measured from the sequence B and the output bits. For Bob, $(d_1, d_2, \ldots, d_m)$ is a completely random binary string. That is, for Bob, each $(d_i \mod 2)$ has an equal chance of being either 0 or 1. In [6], Shannon indicated that unconditional security can only be achieved when the length of the key is at least equal to the length of the plaintext. For ease of analysis, we rewrite the function $r_i = (y_i + y_{i+1} + d_i) \mod 2$ as $r_i = (y_i \oplus y_{i+1}) \oplus (d_i \mod 2)$. This means that the output bits $R \triangleq r_1 r_2 \ldots r_m$ are a completely random binary string for Bob, and therefore, Bob cannot obtain any information about the measurement results and hence cannot deduce x.

For the case of $x = 0$, the Bell state $(|00\rangle + |11\rangle)/\sqrt{2}$ has a density operator of $(|00\rangle + |11\rangle)/\sqrt{2})(\langle 00| + \langle 11|)/\sqrt{2})$. Taking the trace over the second qubit yields the reduced density operator for the first qubit $\rho_{mix} = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2$. For the case of $x = 1$, the qubit sequence B has many possible states. This is because the possible input to the output R is not unique, including the m positions and corresponding measurement bases chosen by Alice, as well as the unpredictable measurement results. Each different combination of parameters can get the same output bits. When Alice announces the unique $R \triangleq r_1 r_2 ... r_m$ based on the measurement results, let the set of all possible states of the qubit sequence B be $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_N\rangle$. Let ρ_x be the reduced density matrix corresponding to the mixture B when classical bit x is committed. Since each qubit of the sequence B is independent of the other, we get

$$\rho_0 = \bigotimes_{i=1}^{n} \rho_{mix} \approx \rho_1 = \sum_{i=1}^{N} \frac{1}{N} |\psi_i\rangle \langle\psi_i|,$$

with

$$|\psi_1\rangle = [\bigotimes_{i=1}^{m} (\frac{1}{2}(|y_i\rangle\langle y_i| + |y_i'\rangle\langle y_i'|) \otimes \mathcal{I}_{\frac{l}{2}-1})] \otimes \mathcal{I}_{n-\frac{ml}{2}},$$

$$|\psi_2\rangle = [\bigotimes_{i=1}^{m} (\frac{1}{2}(|\bar{y}_i\rangle\langle \bar{y}_i| + |\bar{y}_i'\rangle\langle \bar{y}_i'|) \otimes \mathcal{I}_{\frac{l}{2}-1})] \otimes \mathcal{I}_{n-\frac{ml}{2}},$$

$$|\psi_3\rangle = \frac{1}{2}(|y_1\rangle\langle y_1| + |y_1'\rangle\langle y_1'|) \otimes \mathcal{I}_{\frac{l}{2}} \otimes [\bigotimes_{i=2}^{m} (\frac{1}{2}(|\bar{y}_i\rangle\langle \bar{y}_i| + |\bar{y}_i'\rangle\langle \bar{y}_i'|) \otimes \mathcal{I}_{\frac{l}{2}-1})] \otimes \mathcal{I}_{n-\frac{ml}{2}-1},$$

$$|\psi_4\rangle = \frac{1}{2}(|\bar{y}_1\rangle\langle \bar{y}_1| + |\bar{y}_1'\rangle\langle \bar{y}_1'|) \otimes \mathcal{I}_{\frac{l}{2}} \otimes [\bigotimes_{i=2}^{m} (\frac{1}{2}(|y_i\rangle\langle y_i| + |y_i'\rangle\langle y_i'|) \otimes \mathcal{I}_{\frac{l}{2}-1})] \otimes \mathcal{I}_{n-\frac{ml}{2}-1},$$

$$\vdots$$

$$|\psi_{N-1}\rangle = \mathcal{I}_{n-\frac{ml}{2}} \otimes \bigotimes_{i=1}^{m} (\mathcal{I}_{\frac{l}{2}-1} \otimes \frac{1}{2}(|y_i\rangle\langle y_i| + |y_i'\rangle\langle y_i'|)),$$

$$|\psi_N\rangle = \mathcal{I}_{n-\frac{ml}{2}} \otimes \bigotimes_{i=1}^{m} (\mathcal{I}_{\frac{l}{2}-1} \otimes \frac{1}{2}(|\bar{y}_i\rangle\langle \bar{y}_i| + |\bar{y}_i'\rangle\langle \bar{y}_i'|)),$$

such that N is the number of all combinations that satisfy the equation $r_i = (y_i + y_{i+1} + d_i) \bmod 2$ for all $1 \le i \le m$, and $\mathcal{I}_z = \frac{1}{2^z} I^{\otimes z}$, $y_i \in \{0, 1\}$, $y_i' \in \{+, -\}$; If $y_i = 0$, then $y_i' = +$, else $y_i' = -$; $\bar{y}_i$ and $\bar{y}_i'$ are the negations of y_i and y_i', and $(y_1, y_2, ..., y_m)$ is the possible measurement result corresponding to R. The parameter l indicates that on average one qubit may be measured among l qubits, and the probability of the measurement result being 0 or 1 is equal for Bob. Hence the trace distance between ρ_0 and ρ_1 can be arbitrarily small as l increases. Next, we will analyze why Bob is unable to distinguish between these two mixed states.

The indistinguishability of mixed states ρ_0 and ρ_1 when there is only one copy of the mixed state:

Let ρ_0 and ρ_1 be two mixed states, with ρ_0 being the maximum mixed state, i.e.,

$$\rho_0 = \bigotimes_{i=1}^{n} \rho_{mix} = \frac{1}{2^n} I^{\otimes n} = \sum_i \frac{1}{2^n} |\phi_i\rangle\langle\phi_i|,$$

where 2^n is the dimension of the system, $I^{\otimes n}$ is the n-fold tensor product of the identity operator, and $|\phi_i\rangle$ is a set of orthogonal and normalized bases. The other mixed state, ρ_1, is given by

$$\rho_1 = \sum_{i=1}^{N} \frac{1}{N} |\psi_i\rangle \langle\psi_i| = \sum_i p_i |\phi_i\rangle\langle\phi_i|,$$

where $p_i > 0$ is a probability distribution. Furthermore, Alice can choose to measure on the standard or Hadamard basis, each qubit is a mixed state for Bob, and thus $p_i > 0$.

To prove the conclusion, we need to consider the results of arbitrary measurements on these two mixed states. According to the rules of quantum mechanics, a measurement will cause the state function to collapse to some eigenstate. For the mixed state ρ_0, the probability of measuring $|\phi_i\rangle\langle\phi_i|$ is

$$Tr(|\phi_i\rangle\langle\phi_i|\rho_0) = \frac{1}{2^n} Tr(|\phi_i\rangle\langle\phi_i|) = \frac{1}{2^n} > 0.$$

For the mixed state ρ_1, the probability of measuring $|\phi_i\rangle\langle\phi_i|$ is

$$Tr(|\phi_i\rangle\langle\phi_i|\rho_1) = p_i > 0.$$

Although the probabilities are different, each measurement result is possible to come from either ρ_0 or ρ_1, and since there is only one copy of the mixed state, it is impossible to distinguish between these two mixed states when ρ_0 and ρ_1 close to each other. Furthermore, we have the following theorem.

Theorem 2 (Holevo-Helstrom). *In general, the best success probability to discriminate two mixed states represented by ρ_0 and ρ_1 is given by $\frac{1}{2} + \frac{1}{2}(\frac{1}{2} Tr|\rho_0 - \rho_1|)$.*

As l increases, the trace distance $\frac{1}{2} Tr|\rho_0 - \rho_1|$ between ρ_0 and ρ_1, corresponding to different commitment values, can be arbitrarily small from Bob's point of view. Therefore, according to the Holevo-Helstrom theorem, as l increases, the probability that Bob can successfully distinguish between two commitments is arbitrarily close to 1/2.

In summary, based on the principle of superposition, the probability that a dishonest Bob can derive the value of x through the qubit sequence B and the m output bits can be arbitrarily small as l increases. Therefore, $p \notin$ BQP.

2.2 $p \in$ QMA

In this section, we will show that once Alice has made her commitment, i.e., announced the m output bits R, she will not be able to successfully cheat Bob later.

The goal of dishonest Alice's cheating is that she is able to declare any commitment value at will in the opening phase. If Alice chooses x in the commit phase, then Alice would like to have the ability to switch her commitment to $1-x$ in the opening phase. Nevertheless, as a basic principle, we assume that Alice will not employ such a cheating strategy, which has a negligible probability of success and a non-negligible probability of cheating being detected. In other words, Alice will not engage in dishonest operations from which she gets no benefit.

Based on the superposition principle, Alice has no strategy to determine whether the selected qubit a_{j_i} outputs 0 or 1 before measuring it for the case of $x = 1$. Moreover, each selected qubit a_{j_i} output of 0 or 1 is independent, and $Pr(r_i = 0) = Pr(r_i = 1) = 1/2$. If Alice chooses to measure some of the qubits and some of the qubits remain entangled for the selected qubits a_{j_i} $(1 \leq i \leq m)$, then this strategy makes Alice's probability of successfully switching commitment values in the opening phase decrease exponentially as m increases, and the probability of being detected as cheating is non-negligible. Therefore, Alice cannot get any benefit from using such a cheating strategy.

For the case of $x = 0$, the success probability of convincing Bob to accept $x = 1$ decreases exponentially as m increases. In this case, Alice measures the qubits in the opening phase, and since the measurement outcomes are unpredictable, the probability of the output bits matching the previously given random bits (evidence) is only $1/2^m$. Alice may forge the argument y_i to make the equation $r_i = (y_i + y_{i+1} + d_i) \bmod 2$ hold. Without loss of generality, suppose that the measurement basis of a_{j_i} is $k = 0$, and the measurement result is $h = 0$, and then she will announce that $k_{cheat} = 1 \neq k, h_{cheat} = 1 \neq h$. Then the probability that this selected qubit is accepted by Bob (i.e., the probability that the qubit b_{j_i} will be accepted) is $Pr(h' = 1|k' = k_{cheat} \neq k) = 1/2$, where k', h' are Bob's records on qubit b_{j_i}.

To convince Bob to accept $x = 1$, Alice considers forging the measurement result y_i to make the output consistent with the evidence R. The question is how to forge as few qubits measurement results as possible. Assuming that Alice already has measured a_{j_i} and got y_i, now Alice chooses (the best strategy is under the condition $l \leq d_i < \frac{3l}{2}$) to measure the next qubit $a_{j_{i+1}}$ to get y_{i+1}. If $r_i = (y_i + y_{i+1} + d_i) \bmod 2$ holds (with 1/2 probability) for the corresponding r_i in R, then Alice continues to choose to measure the next qubit $a_{j_{i+2}}$. If $r_i = (y_i + y_{i+1} + d_i) \bmod 2$ does not hold, Alice can consider measuring one more qubit backward between a_{j_i} and $a_{j_{i+1}}$ as the new $a_{j_{i+1}}$, and set the original $a_{j_{i+1}}$ to $a_{j_{i+2}}$. According to $r_i = (y_i + y_{i+1} + d_i) \bmod 2$, if Alice chooses to measure one more qubit backward, there are two possible cases, each with probability 1/2: In one case, according to y_{i+1}, Alice has a 1/2 probability of getting two matching output bits (r_i, r_{i+1}), both of which satisfy the equation, and a 1/2 probability of getting two mismatched output bits $(\bar{r}_i, \bar{r}_{i+1})$. In the other case, no matter whether the measurement result is 0 or 1, there is always a measurement result that needs to be forged, i.e., which outputs $(\bar{r}_i, r_{i+1})$ or $(r_i, \bar{r}_{i+1})$. If it is the former, Alice should choose to measure one more qubit backward; if it is the latter, it is better to continue measuring forward instead of measuring one more qubit backward.

As a conclusion, for a given measured qubit $a_{j_{i+1}}$, there are three possible scenarios: 1) The measurement result y_{i+1} happens to output r_i, and Alice does not need to forge. 2) If Alice chooses to measure one more qubit backward, there is a 1/2 probability of output (r_i, r_{i+1}) and no forgery is needed, and a 1/2 probability of output $(\bar{r}_i, \bar{r}_{i+1})$, which requires forging y_{i+1}. 3) If Alice continues measuring forward, the measurement result y_{i+1} needs to be forged. In summary, on average, for each measured qubit, the probability of needing to falsify a measurement result is $5/16 = 1/2\times 0+1/4\times(1/2\times 0+1/2\times 1/2)+1/4\times 1$. For the case of $x = 0$, the success probability of Alice convincing Bob that $x = 1$ in the opening phase is $1/2^{5m/16}$.

For the case of $x = 1$, the success probability of convincing Bob to accept $x = 0$ in the opening phase decreases exponentially as m increases. When Alice announces that she has chosen $x = 0$, Bob will verify whether each qubit pair is still in the Bell state. Each measured qubit will be detected with a probability of 1/2 in the Bell state verification. Therefore, the success probability of Alice's cheating is $1/2^m$.

In summary, the probability of Alice's cheating success decreases exponentially as m increases. Therefore, $p \in \text{QMA}$.

The MLC Attack (no-go theorem): The well-known proof [7,8,9] of the impossibility of unconditionally secure QBC was supposed to be general. However, we will show that it is not general. In fact, in the generality proof of the impossibility of secure quantum bit commitment [9], the authors use a simplified version of Yao's model [10]. It is this simplified version that makes the proof not general.

In [9], pp. 179-180, there is "However, there are two significant distinctions between Yao's model and ours. First, Yao's model deals with mixed initial states whereas we assume that the initial state of each machine is pure. Second, in Yao's model, the user D does two things in each round of the communication: D carries out a measurement on the current mixed state of the portion of the space, $H_D \otimes H_C$, in his/her control and then performs a unitary transformation on $H_D \otimes H_C$. In our model, the measurement step has been eliminated." In fact, not all protocols can be assumed to start from a pure state. For example, if we assume that the protocol starts with pre-shared Bell states (as the proposed scheme), then it is a mixed state from either Alice's or Bob's point of view.

Moreover, regarding the reason why the measurement step can be eliminated, the authors explain that: "Essentially, we give Alice and Bob quantum computers and quantum storage devices. Therefore, they can execute a quantum bit commitment scheme by unitary transformations." This does not make sense. In fact, based on the quantum superposition principle, the measurement is irreversible and the result is unpredictable, while the unitary transformation is reversible. There is an implicit requirement for using the simplified version of Yao's model, i.e., if Alice can get evidence of commitment without the measurement (i.e., can delay the measurement), then the simplified version will perfectly match such a case. However, there are possible schemes (e.g., the proposed scheme) where Alice cannot get valid evidence of commitment without the measurement (That is, not in all cases, Alice can delay the measurement), otherwise, allowing Bob to detect Alice cheating with a probability close to 1 in the opening phase. The inability to delay the measurement makes it impossible for Alice to switch the commitment in the opening phase.

For the proposed scheme, suppose Alice chooses not to measure any qubits during the commit phase (i.e., $x = 0$). The desired effect of this strategy is that Alice can successfully switch the commitment to $x = 1$ with a large probability in the opening phase, which is an MLC EPR-type attack [9]. However, we will prove by reduction to absurdity that if Alice can successfully switch the commitment from $x = 0$ to $x = 1$ with a large probability, then this will lead to the paradoxical result of FTL transmission.

In non-ideal bit commitment (for the case $\rho_0 \neq \rho_1$), the authors describe Alice's attack behavior as follows [9]: "Since $|\psi_0\rangle_{AB}$ and $|1\rangle_{\text{com}}$ are very similar, Bob clearly has a hard time in detecting the dishonesty of Alice. Therefore, Alice can cheat successfully with a very large probability." This means that the state of the sequence B' in the opening phase is very similar or identical to a certain quantum state $|\psi_i\rangle \in \{|\psi_0\rangle, |\psi_1\rangle, ..., |\psi_N\rangle\}$, so Alice can cheat successfully with a very large probability. However, theoretically, when the reduced density matrix of the receiver is ρ_0, the probability of outputting $R \triangleq r_1 r_2 ... r_m$ is $1/2^m$, while the probability of implementing this attack is "a very large probability".

For the sake of simplicity in analysis, let us consider a simplified version of the proposed scheme: set $n = 100$, $m = 2$ and $r_i = y_i \oplus y_{i+1}$, which satisfies the approximate equation $\rho_0 \approx \rho_1$ (ρ_0 and ρ_1 are defined in the following paragraph). Denote the output bits according to the measurement results as $y_1 y_2 \to r_1 r_2$, where $00 \to 00$, $01 \to 11$, $10 \to 11$, and $11 \to 00$. Theoretically, the measurement result y belongs to $\{00, 01, 10, 11\}$ with the same probability.

Suppose Alice chooses not to measure any qubits in the commit phase (i.e., $x = 0$) and claims that $R = 00$. In the opening phase, if Alice can cheat successfully with a large probability, this means she can make the measurement value $y \in \{00, 11\}$ occur with a very high probability and the measurement value $y \in \{01, 10\}$ occur with a very small probability. That is to say, for each sample, Alice has the ability to make its measurement value $y \in \{00, 11\}$ (case $x = 1$) with a probability greater than $1/2$ or simply to keep the Bell states (case $x = 0$). Obviously, the receiver Bob can obtain the density matrix of the sequence B which maintains the Bell states denoted as ρ_0. Moreover, although Bob does not know the measurement bases and positions, he can exhaustively enumerate the states satisfying $R = 00$ with all possible combinations of measurement bases and positions, and obtain the density matrix corresponding to the equal probability of occurrence, denoted as ρ_1. Since ρ_0 and ρ_1 are not exactly equal, there exists a POVM that allows Bob to distinguish them with a non-zero probability ϵ. Although this probability ϵ is small for a single sample, assuming the total number of samples is M, the probability that Bob will never succeed in distinguishing x is $(1-\epsilon)^M$. It can be seen that as the number of samples increases, the probability of Bob successfully distinguishing $1-(1-\epsilon)^M$ will infinitely converge to 1. That is, Bob can figure out Alice's commitment value x, as long as the number of samples is large enough.

That is, if this assumption is true, it means that at some point, Alice can switch between Bell states and $R = 00$ by performing local unitary transformations. For each sample, if Alice wants to send 0 to Bob, she keeps Bell states, otherwise, she switches to $R = 00$. Meanwhile, when there are enough samples (e.g. 1 million samples), Bob can figure out whether Alice sent him a 0 or a 1 without further information exchange, but through POVM measurements. That is, without additional information exchange, Alice can send 1-bit information to Bob through entanglement alone (under the assumption that considers the pre-shared $n = 100$ Bell states as one sample, and suppose Alice and Bob pre-shared 1 million samples). This obviously violates the principle of no faster-than-light communication, so the assumption can not be true. Therefore, it can be concluded that Alice was unable to change her commitment by delaying measurement after the announcement of the evidence.

Finally, we summarize why the delayed measurement entanglement attack strategy cannot successfully attack the proposed scheme, as follows:

1) If this attack strategy is able to attack the proposed scheme effectively, i.e., in the opening phase, Alice is able to switch the commitment from $x = 0$, to $x = 1$. Then, this strategy should also be able to attack a simplified version of the proposed scheme effectively ($n = 100$, $m = 2$ and $r_i = y_i \oplus y_{i+1}$).

2) Then, without any information from Alice, Bob is able to determine whether 0 and 1 are balanced with more than 1/2 probability by measuring and counting, and let the probability be $1/2+\epsilon$.

3) Although, for 1 sample, ϵ is very small, if enough samples are shared between Alice and Bob, say 1 million samples, then Bob can with a probability close to 1 be able to distinguish whether Alice wants to send him a 0 or a 1 (as long as Alice performs local operations for $x = 0$ (or $x = 1$) for all of these 1 million samples).

4) Thus, this directly leads to the fact that Alice and Bob can transmit 1 bit of information between them, just by entanglement, which clearly violates the principle of no FTL communication.

Therefore, it is impossible for Alice to successfully switch her commitment after the commit phase.

3 Conclusion

We prove that BQP $\neq$ QMA. The impact of this result is profound. Based on this scheme, we can get quantum one-way functions (although the existence of classical one-way functions is still unknown). Secure bit commitment has important applications in a number of cryptographic protocols, including secure coin tossing, obvious transfer, zero-knowledge proofs, and secure computation.

References

1. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010.
2. A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation.* USA: American Mathematical Society, 2002.
3. P. H. Eberhard and R. R. Ross, "Quantum field theory cannot provide faster-than-light communication," *Foundations of Physics Letters*, vol. 2, no. 2, pp. 127–149, 1989.
4. G. C. Ghirardi, R. Grassi, A. Rimini, and T. Weber, "Experiments of the epr type involving cp-violation do not allow faster-than-light communication between distant observers," *EPL (Europhysics Letters)*, vol. 6, no. 2, p. 95, 1988.
5. A. Peres and D. R. Terno, "Quantum information and relativity theory," *Reviews of Modern Physics*, vol. 76, no. 1, pp. 93–123, 2004.
6. C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
7. D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Physical Review Letters*, vol. 78, pp. 3414–3417, 1997.
8. H. K. Lo and H. F. Chau, "Is quantum bit commitment really possible?" *Physical Review Letters*, vol. 78, pp. 3410–3413, 1997.
9. ——, "Why quantum bit commitment and ideal quantum coin tossing are impossible," *Physica D: Nonlinear Phenomena*, vol. 120, no. 1-2, pp. 177–187, 1998.
10. A. C.-C. Yao, "Security of quantum protocols against coherent measurements," in *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, 1995, pp. 67–75.