Electronic Colloquium on Computational Complexity, Report No. 103 (2011)

BQP and **PPAD**

Yang Daniel Li

July 31, 2011

Abstract

We initiate the study of the relationship between two complexity classes, **BQP** (**B**ounded-Error **Q**uantum **P**olynomial-Time) and **PPAD** (**P**olynomial **P**arity **A**rgument, **D**irected). We first give a conjecture that **PPAD** is contained in **BQP**, and show a necessary and sufficient condition for the conjecture to hold. Then we prove that the conjecture is not true under the oracle model. In the end, we raise some interesting open problems/future directions.

ISSN 1433-8092

1 Introduction

Quantum computing and algorithmic game theory are two exciting and active areas in the last two decades. Quantum computing lies in the intersection of computer science and quantum physics, and studies the power and limitation of a quantum computer. Algorithmic game theory touches upon the foundations of both computer science and economics, and aims to design efficient algorithms in strategic circumstances. If we want to come up with some examples that are able to demonstrate the interaction between computer science and other disciplines, then quantum computing and algorithmic game theory are two perfect candidates. Quantum mechanics may provide additional computational power, and quantum computers can test the foundations of quantum mechanics. Economics lends some strategic views, and computer science rewards with computational points of view. We refer readers to [NC00] and [NRTV07] for more information.

The central topics of quantum computing and algorithmic game theory are the hardness of two complexity classes, **BQP** (**B**ounded-Error **Q**uantum **P**olynomial-Time) and **PPAD** (**P**olynomial **P**arity **A**rgument, **D**irected). **BQP**, as introduced by Bernstein and Vazarani [BV97], characterizes efficient computation of a quantum computer and is the quantum analog of **BPP**. Very little is known about **BQP**, and a wide belief is that **BQP** and **NP** are incomparable complexity classes [BBBV97, BV97, Aar10]. Papadimitriou introduced the complexity class **PPAD** [Pap94], which is a special class between **P** and **NP**. Since then, the hardness of **PPAD** has also become a longstanding open problem. Although lots of important problems, say the problem of computing a Nash equilibrium (*NASH* for short) [DGP09, CDT09], were shown to be **PPAD**-complete, there have been very few relations from **PPAD** to other complexity classes.

In this paper, we initiate the study of the relationship between **BQP** and **PPAD**. The representative problem of **PPAD** is *NASH* [Pap94], and the most well-known problem in **BQP** is factoring [Sho97]. Both *NASH* and factoring are in the complexity class **TFNP** (the set of total search problems, see [MP91]) in the sense that every instance of *NASH* and factoring always has a solution. Therefore, it seems that there may be some relationship between **PPAD** and **BQP**.

In fact, this possible relation was (implicitly) mentioned in a talk given by Papadimitriou ten years ago [Pap01]. Papadimitrious said that "together with factoring, the complexity of finding a Nash equilibrium is in my opinion the most important concrete open question on the boundary of **P** today". In other words, Papadimitriou asked: do there exist (classically and deterministically) efficient algorithms for factoring and *NASH*? As it have been shown that there exist efficient quantum algorithms for factoring [Sho97], it is natural for us to ask: do there exist efficient quantum algorithms for *NASH*? More generally, is **PPAD** contained in **BQP**?

Our conjecture is that **PPAD** is contained in **BQP**. Formally,

Conjecture 1 **PPAD** $\subseteq$ **BQP**.

The conceived relationship can be illustrated by Figure 1, where the *green+red* is **BQP** and the *red* denotes **PPAD**.

We will formally define quantum Nash equilibrium, the quantum analog of Nash equilibrium, and prove the fact that **PPAD** is contained in **BQP** if and only if there exists a polynomial-time quantum algorithm for computing a quantum Nash equilibrium. Therefore, to prove the conjecture, we need to find an efficient (polynomial-time) quantum algorithm, and to disprove the conjecture, we have to show a super-polynomial lower bound for the time complexity of computing a quantum Nash equilibrium.

Another way to express the conjecture is that quantum computers can compute a Nash equilibrium in polynomial time, or that quantum computers can exponentially speed-up the computation of a Nash equilibrium. And we will rule out this possibility under the oracle model.

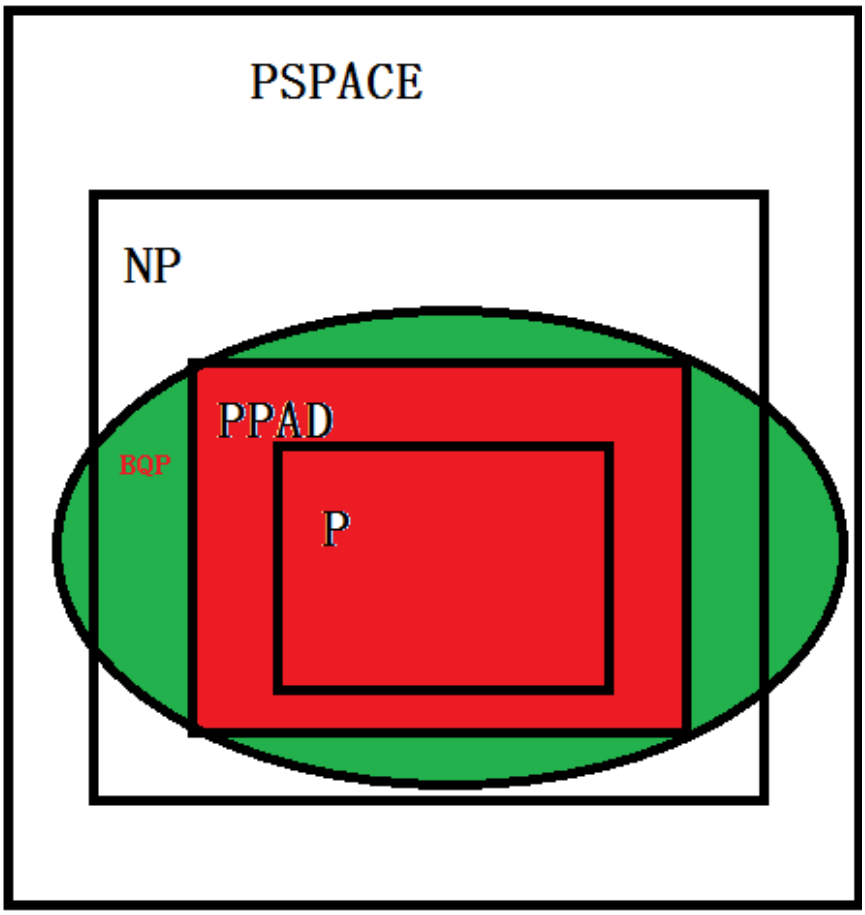

Figure 1: The conceived picture

The organization of this paper is as follows. Section 2 presents the definition of **BQP** and **PPAD**, and in Section 3, we introduce the notion of quantum Nash equilibrium and analyze it. Section 4 provides the necessary and sufficient condition for our conjecture to hold. Section 5 proves a lower bound of computing a Nash equilibrium using quantum computers under the oracle model. And we concludes the paper with some open problems/future directions in Section 6.

2 Preliminaries

2.1 Notation

Some notations used throughout the paper are listed here.

- $\mathbb{N}$: the set of natural numbers, $\{1, 2, 3, \ldots\}$.
- $[n]$: the integer set $\{1, 2, \ldots, n\}$.
- $\mathbb{R}$: the set of real numbers.
- $||\phi||$: the 2-norm of a vector ϕ. If ϕ is a quantum state $\sum_x \alpha_x |x\rangle$, then $||\phi|| = \sqrt{\sum_x |\alpha_x|^2}$.

2.2 BQP

[BV97] introduced the notion of **BQP**, and a simplified version is as follows.

Definition 1 *A language L is in* **BQP** *if and only if there exists a polynomial-time uniform family of quantum circuits $\{Q_n : n \in \mathbb{N}\}$, such that*

- *For all $n \in \mathbb{N}$, Q_n takes n qubits as input and outputs 1 bit.*
- *For all x in L, $Pr(Q_{|x|}(x) = 1) \geq 2/3$.*
- *For all x not in L, $Pr(Q_{|x|}(x) = 0) \geq 2/3$.*

2.3 PPAD and PPAD-completeness

Total search problems are problems for which solutions are guaranteed to exist, and the challenge is to find a specific solution. In [Pap94], Papadimitriou defined the following total search problem.

Definition 2 *(END-OF-THE-LINE) Let S (standing for* **S***uccessor) and P (standing for* **P***redecessor) be two polynomial size circuits that given input strings $\{0,1\}^n$ output strings $\{0,1\}^n$. We further require that $P(0^n) = 0^n \neq S(0^n)$. The aim is to find an input x such that $P(S(x)) \neq x$ or $S(P(x)) \neq x \neq 0$.*

A more intuitive description of END-OF-THE-LINE is as follows. G is a (possibly exponentially large) directed graph with no isolated vertices, and with every vertex having at most one predecessor and one successor. G is specified by giving a polynomial-time computable function $f(v)$ (polynomial in the size of v) that returns the predecessor and successor (if they exist) of the vertex v. Given a vertex s in G with no predecessor, find a vertex $t \neq s$ with no predecessor or no successor. (The input to the problem is the source vertex s and the function $f(v)$). In other words, we want any source or sink of the directed graph other than s.

PPAD was defined based on this problem.

Definition 3 ***(PPAD)*** *The complexity class* **PPAD** *contains all total search problems reducible to END-OF-THE-LINE in polynomial time.*

PPAD-completeness was also defined.

Definition 4 ***(PPAD**-completeness) A problem is called* **PPAD***-complete if it is in* **PPAD** *and all problems in* **PPAD** *can reduce to it in polynomial time.*

3 Quantum Nash Equilibrium

3.1 Classical Equilibria

First, we review classical Nash equilibria and correlated equilibria, all of which can be found in [NRTV07].

In a classical game there are n players, labeled $\{1, 2, \ldots, n\}$. Each player i has a set S_i of strategies. We use $s = (s_1, \ldots, s_n)$ to denote the vector of strategies selected by the players and $S = \times_i S_i$ to denote the set of all possible joint strategies. Each player i has a utility function $u_i : S \to \mathbb{R}$, giving the payoff or utility $u_i(s)$ to player i on the joint strategy s. There is a solution concept called Nash equilibrium, in which the equilibrium strategies are known by all players, and no player can gain more by unilaterally modifying his or her choice. Formally,

Definition 5 *A* mixed Nash equilibrium *is a probability vector $p = p_1 \times \ldots \times p_n$ for some probability distributions p_i's over S_i's satisfying that*

$$\sum_{s_{-i}} p_{-i}(s_{-i}) u_i(s_i, s_{-i}) \geq \sum_{s_{-i}} p_{-i}(s_{-i}) u_i(s'_i, s_{-i}), \qquad \forall i \in [n], \forall s'_i \in S_i, \forall s_i \in S_i \text{ s.t. } p_i(s_i) > 0,$$

where s_{-i} is the strategies chosen by players but player i, and p_{-i} denotes the probability distribution over s_{-i}. Informally speaking, for a mixed Nash equilibrium, the expected payoff over probability distribution of s_{-i} is maximized, i.e. $\mathbf{E}_{s_{-i}}[u_i(s_i, s_{-i})] \geq \mathbf{E}_{s_{-i}}[u_i(s'_i, s_{-i})]$.

We can further relax the Nash condition and define an ϵ-approximate Nash equilibrium to be a profile of mixed strategies such that no player can gain more than ϵ amount by changing his/her own strategy unilaterally. Formally,

Definition 6 *An* ϵ-approximate Nash equilibrium *is a probability vector* $p = p_1 \times \ldots \times p_n$ *for some probability distributions* p_i*'s over* S_i*'s satisfying that*

$$\sum_{s_{-i}} p_{-i}(s_{-i})u_i(s_i, s_{-i}) \geq \sum_{s_{-i}} p_{-i}(s_{-i})u_i(s'_i, s_{-i}) - \epsilon, \qquad \forall i \in [n], \forall s'_i \in S_i, \forall s_i \in S_i \text{ s.t. } p_i(s_i) > 0,$$

where $\epsilon > 0$. In addition, the probability distribution of each player may not be independent, but correlated, forming the notion of correlated equilibria.

Definition 7 *A* correlated equilibrium *is a probability distribution* p *over* S *satisfying that*

$$\sum_{s_{-i}} p(s_i, s_{-i})u_i(s_i, s_{-i}) \geq \sum_{s_{-i}} p(s_i, s_{-i})u_i(s'_i, s_{-i}), \qquad \forall i \in [n], \forall s_i, s'_i \in S_i.$$

Notice that a correlated equilibrium p is a Nash equilibrium if and only if p is a product distribution.

3.2 Quantum Equilibria

This part generalizes classical equilibria to quantum equilibria, where players are allowed to use "quantum" strategies. To be more precise, each player i now has a Hilbert space $H_i = span\{s_i : s_i \in S_i\}$, and the joint strategy can be any quantum state ρ in $H = \otimes_i H_i$. The payoff/utility for player i on joint strategy ρ is $\mu_i(\rho) = \mathbf{E}[u_i(s(\rho))] = \sum_s \langle s|\rho|s\rangle u_i(s)$, where $s(\rho)$ is the outcome pure strategy when ρ is measured according to the computational basis $\{s : s \in S\}$. Note that what each player i can do is to apply an admissible super-operator Φ_i on her own space H_i. We sometimes write Φ_i for $\Phi_i \otimes I_{-i}$. We use $CPTP(X)$ to denote the set of all admissible (completely positive and trace preserving) super-operators on a space X. The notions of quantum Nash equilibria and quantum correlated equilibria are defined as follows.

Definition 8 *A* quantum Nash equilibrium *is a quantum strategy* $\rho = \rho_1 \otimes \ldots \otimes \rho_n$ *for* ρ_i*'s in* H_i*'s satisfying*

$$\sum_s \langle s|\rho|s\rangle u_i(s) \geq \sum_s \langle s|\Phi_i(\rho)|s\rangle u_i(s), \qquad \forall i \in [n], \forall \Phi_i \in CPTP(H_i)$$

Definition 9 *A* quantum correlated equilibrium *is a quantum strategy* ρ *in* H *satisfying*

$$\sum_s \langle s|\rho|s\rangle u_i(s) \geq \sum_s \langle s|\Phi_i(\rho)|s\rangle u_i(s), \qquad \forall i \in [n], \forall \Phi_i \in CPTP(H_i)$$

3.3 Relations between Classical and Quantum Equilibria

This section studies the relation between classical and quantum equilibria. A quantum mixed state ρ naturally induces a classical distribution p over S defined by

$$p(s) = \rho_{ss} \tag{1}$$

While taking diagonal entries seems to be the most natural mapping from quantum states to classical distributions, there are more options for the mapping in other direction. Given a classical distribution p over S, we can consider

1. $\rho(p) = \sum_s p(s)|s\rangle\langle s|$,
2. $|\psi(p)\rangle = \sum_s \sqrt{p(s)}|s\rangle$, or
3. any density matrix ρ with $p(s) = \rho_{ss}$ satisfied.

We want to study whether equilibria in one world, classical or quantum, implies equilibria in the other world. The following theorem says that quantum always implies classical.

Theorem 3.1 *If ρ is a quantum correlated equilibrium, then p defined by $p(s) = \rho_{ss}$ is a classical correlated equilibrium. In particular, if ρ is a quantum Nash equilibrium, then p is a classical Nash equilibrium.*

Proof: See the appendix. □

The implication from classical to quantum is much more complicated. The following theorem says that the first mapping always gives a quantum equilibrium. That is, the utility of i cannot be increased for a classical equilibrium even when player i is allowed to have quantum operations.

Theorem 3.2 *If p is a classical correlated equilibrium, then $\rho = \Sigma_{s\in S}|s\rangle\langle s|$ is a quantum correlated equilibrium. In particular, if p is a classical Nash equilibrium, then ρ as defined is a quantum Nash equilibrium.*

Proof: See the appendix. □

Following this result, we are able to give an affirmative answer to an important problem, whether quantum Nash equilibria always exist.

Corollary 3.3 *For all standard game G with finite number of players and strategies, quantum Nash equilibria always exist.*

Proof: See the appendix. □

The second way of inducing a quantum state is interesting: It preserves (uncorrelated) Nash equilibria, but does not preserve correlated Nash equilibria in general.

Theorem 3.4 *There exists a classical correlated equilibrium p with $|\psi\rangle = \sum_s \sqrt{p(s)}|s\rangle$ not being a quantum correlated equilibrium. However, if p is a classical Nash equilibrium, then $|\psi\rangle = \sum_s \sqrt{p(s)}|s\rangle$ is a quantum Nash equilibrium.*

Proof: See the appendix. □

Finally, for the third mapping, *i.e.* a general ρ with $p(s) = \rho_{ss}$ satisfied, the equilibrium property can be heavily destroyed, even if p is uncorrelated. (Actually, we will show such counterexamples even for two-player symmetric games.)

Theorem 3.5 *There exist ρ and p satisfying that $p(s) = \rho_{ss}$, p is a classical Nash equilibrium, but ρ is not even a quantum* correlated *equilibrium.*

Proof: See the appendix. □

Despite of the above fact, one should not think that the large range of the third type of mappings always enables some mapping to destroy the equilibria.

Theorem 3.6 *There exist classical correlated equilibria p, such that all quantum states ρ with $\rho_{ss} = p(s)$ are quantum correlated equilibria.*

Proof: See the appendix. □

4 A Necessary and Sufficient Condition

In this section, we prove the following theorem.

Theorem 4.1 **PPAD** $\subseteq$ **BQP** *if and only if there exists a polynomial-time quantum algorithm for finding a quantum Nash equilibrium.*

Proof:

If **PPAD** $\subseteq$ **BQP**, then for a game G, there exists a polynomial-time quantum algorithm for finding a Nash equilibrium p, since finding a Nash equilibrium is a **PPAD**-complete problem. As shown in the proof of Corollary 3.3, we can always convert p to a quantum equilibrium ρ

in polynomial time. Hence, there exists a polynomial-time quantum algorithm for finding a quantum Nash equilibrium.

Next we will prove the inverse direction for the statement.

We define a new problem as follows.

Definition 10 *SAMPLE-NASH is a search problem that, on input a game G, outputs a pure strategy s sampled from a fixed Nash equilibrium p of the game G.*

Suppose that we are given a game G and we find a quantum Nash equilibrium ρ in polynomial-time using the quantum algorithm. Here we assume that the induced classical probability distribution induced from ρ is p, defined by $p(s) = \rho_{ss}$. By measuring ρ according to the computational basis $\{s : s \in S\}$, we can obtain a pure strategy s, which is sampled according to p. According to Theorem 3.1, p is a classical Nash equilibrium, and therefore s is an output for *SAMPLE-NASH*. So we are able to obtain the output for *SAMPLE-NASH* in polynomial time. Now we have a polynomial-time quantum algorithm for *SAMPLE-NASH*.

We have the following result, which is to be proved later.

Lemma 4.2 *A* **PPAD***-complete problem can be reduced to SAMPLE-NASH in randomized polynomial time.*

Therefore, we have a polynomial-time quantum algorithm for a **PPAD**-complete problem, implying **PPAD** $\subseteq$ **BQP**.

□

4.1 Proof of Lemma 4.2

To prove Lemma 4.2, we use the following result.

Lemma 4.3 *[CDT09]*
For any constant $c > 0$, the problem of computing a $1/m^c$-approximate Nash equilibrium of a positively normalized [1] *$m \times m$ bimatrix game is* **PPAD***-complete.*

We just need to reduce the problem in Lemma 4.3, to *SAMPLE-NASH* in randomized polynomial time.

For an instance of the problem in Lemma 4.3, namely a positively normalized $m \times m$ bimatrix game G, we use G as the input for *SAMPLE-NASH*. We assume that we have an algorithm A for *SAMPLE-NASH*, and we want to use A to construct an algorithm for the problem in Lemma 4.3 in randomized polynomial time. Suppose the output of A is sampled from a Nash equilibrium $p = p_1 \times p_2$.

Lemma 4.4 *Suppose that $p = p_1 \times p_2$ is a Nash equilibrium of a positively normalized $m \times m$ bimatrix game G, and that the output of A, an algorithm for SAMPLE-NASH, is sampled from p. For any $\epsilon = O(1/m^c)$, with high probability, we will get a probability distribution $q = q_1 \times q_2$ with $||q_1 - p_1||_1 \leq \epsilon$ and $||q_2 - p_2||_1 \leq \epsilon$, after running A for $O(m^2\epsilon^{-2})$ times.*

Lemma 4.5 *Suppose that $p = p_1 \times p_2$ is a Nash equilibrium of a positively normalized $m \times m$ bimatrix game G. Any probability distribution $q = q_1 \times q_2$ with $||q_1 - p_1||_1 \leq \epsilon$ and $||q_2 - p_2||_1 \leq \epsilon$, is a 2ϵ-approximate Nash equilibrium of game G.*

By Lemma 4.4, we can run algorithm A for $O(m^2\epsilon^{-2})$ times to construct a desired probability distribution q with high probability. By Lemma 4.5, q is an 2ϵ-approximate Nash equilibrium. To find an $1/m^c$-approximate Nash equilibrium, we need to use A for $O(m^{2c+2})$ times, which is polynomial in input size $2m^2$.

[1] In [CDT09], the game matrices are normalized in the sense that all the entries are between 0 and 1 (positively normalized), or between -1 and 1.

4.1.1 Proof of Lemma 4.4

We assume that player 1's m strategies are $s_1, s_2, \ldots, s_m$. Define $k = \lceil 4000m^2/\epsilon^2 \rceil = O(m^2\epsilon^{-2})$. For each $i \in [k]$, $j \in [m]$, define random variable X_{ij} taking values in $\{0, 1\}$, where $X_{ij} = 1$ with probability $p_1(s_j)$.

Suppose that $\epsilon_j = \frac{\epsilon}{2m}$ for each $j \in [m]$. Define random variables X_j to be $X_j = \frac{\sum_{i\in[k]} X_{ij}}{k}$ for each $j \in [m]$. By Chernoff bound,

$$Pr(X_j \geq p_1(s_j) + \epsilon_j) \leq e^{-2\epsilon_j^2 k} \tag{2}$$

and

$$Pr(X_j \leq p_1(s_j) - \epsilon_j) \leq e^{-2\epsilon_j^2 k}. \tag{3}$$

Define a probability vector q_1 to be $(X_1, \ldots, X_m)$, which is a distribution over strategies $(s_1, s_2, \ldots, s_m)$. It is easily checkable that $\sum_j X_j = 1$ and that

$$\begin{aligned} Pr(||q_1 - p_1||_1 \leq \sum_{j\in[m]} |X_j - p_1(s_j)| \leq \sum_{j\in[m]} \epsilon_j \leq \epsilon) &\geq 1 - \sum_{j\in[m]} 2e^{-2\epsilon_j^2 k} &(4)\\ &\geq 0.995. &(5)\end{aligned}$$

Similarly, we can get q_2 satisfying $||q_2 - p_2||_1 \leq \epsilon$ with probability at least 0.995. By union bound, we can get the desired q with probability at least 0.99.

4.1.2 Proof of Lemma 4.5

For all i in $\{1, 2\}$, for all s_i' in the set of strategies of player i, and for all s_i in the support of the set of strategies of player i, we have the following:

$$\begin{aligned}
&\sum_{s_{-i}} q_{-i}(s_{-i})u(s_i' s_{-i}) - \sum_{s_{-i}} q_{-i}(s_{-i})u(s_i s_{-i})\\
=&\sum_{s_{-i}} p_{-i}(s_{-i})u(s_i' s_{-i}) + \sum_{s_{-i}} (q_{-i}(s_{-i}) - p_{-i}(s_{-i}))u(s_i' s_{-i}) - \sum_{s_{-i}} q_{-i}(s_{-i})u(s_i s_{-i})\\
\leq&\sum_{s_{-i}} p_{-i}(s_{-i})u(s_i s_{-i}) + ||q_{-i} - p_{-i}||_1 \max_s u(s) - \sum_{s_{-i}} q_{-i}(s_{-i})u(s_i s_{-i})\\
\leq&\sum_{s_{-i}} p_{-i}(s_{-i})u(s_i s_{-i}) + \epsilon \times 1 - \sum_{s_{-i}} q_{-i}(s_{-i})u(s_i s_{-i})\\
\leq&\sum_{s_{-i}} (p_{-i}(s_{-i}) - q_{-i}(s_{-i}))u(s_i s_{-i}) + \epsilon\\
\leq&||q_{-i} - p_{-i}||_1 \max_s u(s) + \epsilon\\
\leq&\epsilon \times 1 + \epsilon\\
\leq&2\epsilon
\end{aligned}$$

Following the definition of approximate Nash equilibrium, q is a 2ϵ-approximate Nash equilibrium of G.

5 A Lower Bound under the Oracle Model

5.1 The Oracle Model

The oracle model is also called black-box model, or relativized model, and is one of simplest models in computer science. Suppose that there is a boolean function $f : [N] \to \{0, 1\}$, and

that f can be computed in polynomial time. We want to find an $x \in [N]$, such that $f(x) = 1$. In the context of **PPAD**-complete problems, N, which could be exponential in the size of the input, is the number of points in the search space, and $f(x) = 1$ for $x \in [N]$ means that x is the answer we desire. For a **PPAD**-complete problem, there always exists an $x \in [N]$, such that $f(x) = 1$, and the question is that we do not know where it is. Such an f is called an oracle, and we want to compute an $x \in [N]$, such that $f(x) = 1$.

In an oracle model, algorithms are allowed to make queries to the oracle but are prohibited to take advantage of what underlies the oracle. Since we use quantum algorithms here, we can also make use of quantum superposition. For instance, for a quantum state $\sum_x \alpha_x |x\rangle$, we first add some ancilla qubits, obtaining $\sum_x \alpha_x |x\rangle|0\rangle$, and then make a single query to the oracle, getting $\sum_x \alpha_x |x\rangle|f(x)\rangle$.

In summary, in the oracle model, the function f can be seen as the input, and we need to design a quantum algorithm to find a solution $x \in [N]$ with $f(x) = 1$, which is guaranteed to exist. The time complexity is what we care and is defined to the number of queries made to the oracle.

5.2 The Lower Bound

We use a hybrid argument of [BBBV97, Vaz04] to show a result when there is only one $x \in [N]$ such that $f(x) = 1$, namely for the problems with a single solution. Hybrid argument is from a classic paper by Yao [Yao82], and later has numerous applications in cryptography and complexity theory [BM84, GL89, HILL99, INW94, Nis91, Nis92, NW94]. Thus, our proof is not new, and existing techniques are enough to prove the result. This is partly due to the fact that the oracle model is very well-studied.

Theorem 5.1 *Under the oracle model, to solve a* **PPAD***-complete problem with a single solution, any quantum algorithm has to make at least* $\Omega(\sqrt{N})$ *queries to the oracle.*

Proof:

Suppose A is an (arbitrary) algorithm under the oracle model, and it makes k queries to the input oracle. If $k = \Omega(N)$, then everything is done and we need to do nothing. So a reasonable assumption is that $k = o(N)$.

We define an auxiliary oracle function $h : [N] \to \{0, 1\}$ with $h(y) = 0$ for all $y \in [N]$. Such an oracle cannot characterize any **PPAD**-complete problem, as there are always solutions for **PPAD**-complete problems while here h means no solution at all. So we use h just purely for analysis.

Run A on h and we call such a run A_h. Let $\sum_{y:y\in[N]} \alpha_{y,t} |y\rangle$ be the query at time $t \in [k]$, and let the query magnitude of y to be $\sum_{t\in[k]} |\alpha_{y,t}|^2$. It is not hard to see that the expected query magnitude over all possible y is $E_y(\sum_t |\alpha_{y,t}|^2) = k/N$. We have the following claim.

Claim 1 *There exist* $z_1, z_2 \in [N]$ *with* $z_1 \neq z_2$*, such that* $\sum_t |\alpha_{z_1,t}|^2 \leq (k+1)/N$ *and* $\sum_t |\alpha_{z_2,t}|^2 \leq (k+1)/N$.

By Cauchy-Schwartz inequality, we know that $\sum_t |\alpha_{z_1,t}| \leq (k+1)/\sqrt{N}$ and that $\sum_t |\alpha_{z_2,t}| \leq (k+1)/\sqrt{N}$.

Let $\phi_{h,t}$, $t \in [k]$ be the states of A_h after the t-th step. We define two oracles $g_1 : [N] \to \{0, 1\}$ and $g_2 : [N] \to \{0, 1\}$:

- $g_1(z_1) = 1$ and for all $y \neq z_1$, $g_1(y) = 0$;
- $g_2(z_2) = 1$ and for all $y \neq z_2$, $g_2(y) = 0$.

g_1 and g_2 are the legal inputs of A and correspond to **PPAD**-complete problems. Now run the algorithm A on g_1 (the run is denoted as A_{g_1}) and suppose the final state of A_{g_1} is $\phi_{g_1,k}$. By hybrid argument, we have the following claim.

Claim 2 *[Vaz04]*
$\phi_{h,k} - \phi_{g_1,k} = \sum_{t=1}^{k} E_t$, *where* $||E_t|| \leq \sqrt{2}|\alpha_{z_1,t}|$.

Along with the triangle inequality, we have

$$\begin{aligned} ||\phi_{h,k} - \phi_{g_1,k}|| &\leq \sum_t ||E_t|| \\ &\leq \sqrt{2}\sum_t |\alpha_{z,t}| \\ &\leq (k+1)\sqrt{2/N}. \end{aligned} \tag{6}$$

Similarly, if we run the algorithm A on g_2 (the run is denoted as A_{g_2}) and the final state of A_{g_2} is $\phi_{g_2,k}$, then a hybrid argument and the triangle inequality could show that

$$||\phi_{h,k} - \phi_{g_2,k}|| \leq (k+1)\sqrt{2/N}. \tag{7}$$

If we apply the triangle inequality for another time, we get

$$||\phi_{g_1,k} - \phi_{g_2,k}|| \leq 2(k+1)\sqrt{2/N}, \tag{8}$$

implying that $\phi_{g_1,k}$ and $\phi_{g_2,k}$ can be distinguished with probability at most $O(k/\sqrt{N})$. Since $z_1 \neq z_2$, if A can solve problems corresponding to g_1 and g_2, namely if A can find z_1 and z_2, it should at least distinguish g_1 and g_2, and also $\phi_{g_1,k}$ and $\phi_{g_2,k}$ with some constant probability. As a result, A should at least make $\Omega(\sqrt{N})$ queries.

□

When there are multiple solutions, say p solutions, then $k = \Omega(\sqrt{N/p})$, which is a straightforward generalization from the theorem above. More formally,

Corollary 5.2 *Under the oracle model, to solve a* **PPAD***-complete problem with p solutions, any quantum algorithm has to make at least $\Omega(\sqrt{N/p})$ queries to the oracle.*

5.2.1 Proof of Claim 1

Let us suppose that there does not exist $z_1, z_2 \in [N]$ with $z_1 \neq z_2$, such that $\sum_t |\alpha_{z_1,t}|^2 \leq (k+1)/N$ and $\sum_t |\alpha_{z_2,t}|^2 \leq (k+1)/N$. This means there is at most one $z \in [N]$ such that $\sum_t |\alpha_{z,t}|^2 \leq (k+1)/N$, and for all $y \neq z$, $y \in [N]$, $\sum_t |\alpha_{y,t}|^2 > (k+1)/N$. Thus,

$$\begin{aligned} \sum_{y:y\in[N]} \sum_t |\alpha_{y,t}|^2 &= \sum_{y:y\neq z} \sum_t |\alpha_{y,t}|^2 + \sum_t |\alpha_{z,t}|^2 \\ &\geq \sum_{y:y\neq z} \sum_t |\alpha_{y,t}|^2 \\ &> (N-1) \times (k+1)/N \\ &= k + 1 - (k+1)/N \\ &> k. \end{aligned} \tag{9}$$

But we have already known that

$$E_{y:y\in[N]}(\sum_t |\alpha_{y,t}|^2) = k/N, \tag{10}$$

and that

$$\sum_{y:y\in[N]} (\sum_t |\alpha_{y,t}|^2) = k. \tag{11}$$

The inequality (9) and the equation (11) exhibit clear contradiction. Consequently, our assumption that there does not exist $z_1, z_2 \in [N]$ with $z_1 \neq z_2$, such that $\sum_t |\alpha_{z_1,t}|^2 \leq (k+1)/N$ and $\sum_t |\alpha_{z_2,t}|^2 \leq (k+1)/N$ is incorrect. This completes the proof of Claim 1.

6 Concluding Remarks

On the one hand, it seems that the well-studied oracle model presents us an insurmountable obstacle towards an exponentially speed-up using quantum computers for computing **PPAD**-complete problems. If we want to make a step closer to prove our conjecture that **PPAD** is contained in **BQP**, we have to get rid of oracles and design new structures that can provide more information. We believe that this may need fundamental revolution in the field of quantum computing. The theory community has spent lots of effort in designing quantum algorithms for factoring as well as graph isomorphism, two special problems between **P** and **NP**. And now it is the time that we turn our attention to the third special problem, *NASH*, or more generally **PPAD**-complete problems.

On the other hand, it seems that purely exploiting the potential of quantum superposition is not enough, and quantum entanglement may play a more important role as a resource for quantum computation. It is well-known that quantum information theory relies on entanglement in two quite different contexts: as a resource for quantum computation and as a source for nonlocal correlations among different parties. It is strange and not understood that entanglement is crucially linked with nonlocality but not with computation. Quantum computation and nonlocality are two faces of entanglement, and more connections should be established in the future.

7 Acknowledgments

Thanks to Shengyu Zhang for discussions at the early stage of this work.

References

[Aar10] Scott Aaronson. BQP and the polynomial hierarchy. *Proceedings of the 42nd Annual ACM symposium on Theory of Computing*, 2010.

[BBBV97] Charles Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[BM84] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Comput.*, 13(4):850–864, 1984.

[BV97] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[CDT09] Xi Chen, Xiaotie Deng, and Shang-Hua Teng. Settling the complexity of computing two-player Nash equilibria. *Journal of ACM*, 56, 2009.

[DGP09] Constantinos Daskalakis, Paul Goldberg, and Christos Papadimitriou. The complexity of computing a Nash equilibrium. *SIAM Journal on Computing*, 39(1):195–259, 2009.

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *STOC*, pages 25–32, 1989.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[INW94] Russell Impagliazzo, Noam Nisan, and Avi Wigderson. Pseudorandomness for network algorithms. In *STOC*, pages 356–364, 1994.

[MP91] Nimrod Megiddo and Christos Papadimitriou. On total functions, existence theorems, and computational complexity. *Theoretical Computer Science*, 81(2):317 –324, 1991.

[NC00] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Nis91] Noam Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica*, 11(1):63–70, 1991.

[Nis92] Noam Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992.

[NRTV07] Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay Vazirani. *Algorithmic Game Theory*. Cambridge University Press, 2007.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994.

[Pap94] Christos Papadimitriou. On the complexity of the parity argument and other inefficient proofs of existence. *Journal of Computer and System Sciences*, 48(3):498–532, 1994.

[Pap01] Christos H. Papadimitriou. Algorithms, games, and the internet. In *STOC*, pages 749–753, 2001.

[Sho97] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[Vaz04] Umesh Vazirani, 2004. Lecture Notes of Quantum Computing.

[Yao82] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *FOCS*, pages 80–91, 1982.

A Proof of Theorem 3.1

Recall that we are given that $\mu_i(\rho) \geq \mu_i(\Phi_i(\rho))$ for all players i and all admissible super-operators Φ_i on H_i, and we want to prove that for all players i and all strategies $s_i, s_i' \in S_i$,

$$\sum_{s_{-i}} p(s_i, s_{-i}) u_i(s_i, s_{-i}) \geq \sum_{s_{-i}} p(s_i, s_{-i}) u_i(s_i', s_{-i}) \tag{12}$$

for $p(s) = \rho_{ss}$.

Fix i and s_i, s_i'. Consider the admissible super-operator Φ_i defined by

$$\Phi_i = \sum_{t_i \neq s_i} P_{t_i} \rho P_{t_i} + (s_i \leftrightarrow s_i') P_{s_i} \rho P_{s_i} (s_i \leftrightarrow s_i') \tag{13}$$

where P_{t_i} is the projection onto the subspace $span(t_i) \otimes H_{-i}$, and $(s_i \leftrightarrow s_i')$ is the operator swapping s_i and s_i'. It is not hard to verify that Φ_i is an admissible super-operator. Next we will show that the difference of $\mu_i(\rho)$ and $\mu_i(\Phi_i(\rho))$ is the same as that of the two sides of Eq. (12).

$$\begin{aligned}
\mu_i(\rho) &= \mathbf{E}[u_i(s(\rho))] \\
&= \sum_{\bar{s} \in S} \langle \bar{s} | \rho | \bar{s} \rangle u_i(\bar{s}) = \sum_{\bar{s} \in S} p(\bar{s}) u_i(\bar{s}) \\
&= \sum_{\bar{s}_i \neq s_i} \sum_{\bar{s}_{-i}} p(\bar{s}) u_i(\bar{s}) + \sum_{\bar{s}_{-i}} p(s_i \bar{s}_{-i}) u_i(s_i \bar{s}_{-i})
\end{aligned} \tag{14}$$

$$\begin{aligned}
\mu_i(\Phi_i(\rho)) &= \sum_{\bar{s} \in S} \langle \bar{s} | \Phi_i(\rho) | \bar{s} \rangle u_i(\bar{s}) \\
&= \sum_{\bar{s} \in S} \langle \bar{s} | \sum_{t_i \neq s_i} P_{t_i} \rho P_{t_i} + (s_i \leftrightarrow s_i') P_{s_i} \rho P_{s_i} (s_i \leftrightarrow s_i') | \bar{s} \rangle u_i(\bar{s}) \\
&= \sum_{\bar{s} \in S} \langle \bar{s} | \sum_{t_i \neq s_i} P_{t_i} \rho P_{t_i} | \bar{s} \rangle u_i(\bar{s}) + \sum_{\bar{s} \in S} \langle \bar{s} | (s_i \leftrightarrow s_i') P_{s_i} \rho P_{s_i} (s_i \leftrightarrow s_i') | \bar{s} \rangle u_i(\bar{s}) \\
&= \sum_{t_i \neq s_i} \sum_{\bar{s}_{-i}} p(t_i \bar{s}_{-i}) u_i(t_i \bar{s}_{-i}) + \sum_{\bar{s}_{-i}} p(s_i \bar{s}_{-i}) u_i(s_i' \bar{s}_{-i})
\end{aligned} \tag{15}$$

Since ρ is a quantum correlated equilibrium, we have $\mu_i(\rho) \geq \mu_i(\Phi_i(\rho))$. Comparing the above two expressions for $\mu_i(\rho)$ and $\mu_i(\Phi_i(\rho))$ gives Eq. (12) as desired.

B Proof of Theorem 3.2

Let $\alpha(s_i) = \sum_{s_{-i}} p(s_i, s_{-i}) u_i(s_i, s_{-i})$ and $\beta(s_i, s_i') = \sum_{s_{-i}} p(s_i, s_{-i}) u_i(s_i', s_{-i})$. Now for any i, we have

$$\mu_i(\rho) = \sum_s \langle s | \rho | s \rangle u_i(s) = \sum_s p(s) u_i(s) = \sum_{s_i} \sum_{s_{-i}} p(s_i s_{-i}) u_i(s_i s_{-i}) = \sum_{s_i} \alpha(s_i) \tag{16}$$

where the first two steps are by the definition of μ_i and p. Now for an arbitrary TPCP super-operator Φ_i, we use its Kraus representation to obtain

$$\Phi_i(\rho) = \sum_{j=1}^{k} (A_{ij} \otimes I_{-i}) \rho (A_{ij}^* \otimes I_{-i}) \tag{17}$$

with constraint $\sum_{j=1}^{k} A_{ij}^* A_{ij} = I_i$, where I_i is the identity super-operator from $L(H_i)$ to $L(H_i)$. Now we have

$$\begin{aligned}
\mu_i(\Phi_i(\rho)) &= \sum_{s'} \langle s'|\Phi_i(\rho)|s'\rangle u_i(s') \qquad \text{// by the def of } \mu_i \\
&= \sum_{s'} \langle s'| \sum_{j=1}^{k} (A_{ij} \otimes I_{-i}) \rho (A_{ij}^* \otimes I_{-i}) |s'\rangle u_i(s') \\
&= \sum_{s'} \sum_{j=1}^{k} \langle s'|(A_{ij} \otimes I_{-i})(\sum_{s} p(s)|s\rangle\langle s|)(A_{ij}^* \otimes I_{-i})|s'\rangle u_i(s') \qquad \text{// by the def of } \rho \\
&= \sum_{s'} \sum_{s} \sum_{j=1}^{k} \langle s'|A_{ij} \otimes I_{-i}|s\rangle\langle s|A_{ij}^* \otimes I_{-i}|s'\rangle p(s) u_i(s') \\
&= \sum_{s'_i} \sum_{s} \sum_{j=1}^{k} \langle s'_i|A_{ij}|s_i\rangle\langle s_i|A_{ij}^*|s'_i\rangle p(s_i s_{-i}) u_i(s'_i s_{-i}) \\
&= \sum_{s'_i} \sum_{s_i} \sum_{j=1}^{k} \langle s'_i|A_{ij}|s_i\rangle\langle s_i|A_{ij}^*|s'_i\rangle \beta(s_i, s'_i) \qquad \text{// by the def of } \beta(s_i, s'_i)
\end{aligned}$$

Note that $\langle s'_i|A_{ij}|s_i\rangle\langle s_i|A_{ij}^*|s'_i\rangle = \|\langle s'_i|A_{ij}|s_i\rangle\|^2 \geq 0$, thus by the assumption that $\beta(s_i, s'_i) \leq \alpha(s'_i)$ (i.e. p is a classical correlated equilibrium), we have

$$\begin{aligned}
\mu_i(\Phi_i(\rho)) &\leq \sum_{s_i} \sum_{j=1}^{k} \sum_{s'_i} \langle s'_i|A_{ij}|s_i\rangle\langle s_i|A_{ij}^*|s'_i\rangle \alpha(s_i) \\
&= \sum_{s_i} \sum_{j=1}^{k} \langle s_i|A_{ij}^*(\sum_{s'_i} |s'_i\rangle\langle s'_i|) A_{ij}|s_i\rangle \alpha(s_i) \\
&= \sum_{s_i} \langle s_i| \sum_{j=1}^{k} A_{ij}^* A_{ij} |s_i\rangle \alpha(s'_i) \\
&= \sum_{s_i} \langle s_i|s_i\rangle \alpha(s_i) \\
&= \mu_i(\rho)
\end{aligned}$$

where the last equality is by Eq. (16). This completes the proof of Theorem 3.2.

B.1 Proof of Corollary 3.3

We will reduce the existence of a quantum Nash equilibrium to the existence of a Nash equilibrium.

For a given game G with finite players and finite strategies, there always exists a Nash equilibrium, say p. We transform p into a quantum state ρ using the the mapping $\rho = \sum_s p(s)|s\rangle\langle s|$. By Theorem 3.2, ρ is guaranteed to be quantum Nash equilibrium of G.

Thus, quantum Nash equilibria always exist.

C Proof of Theorem 3.4

C.1 Examples of the First Statement

Define utility functions of Player 1 and 2 to be:

$$A = \begin{bmatrix} 270 & 126 \\ 0 & 270 \end{bmatrix}.$$

Suppose the initial state is

$$|\psi\rangle = \sqrt{1/3}|00\rangle + \sqrt{1/6}|01\rangle + \sqrt{1/6}|10\rangle + \sqrt{1/3}|11\rangle,$$

whose corresponding density matrix is

$$\rho = \begin{bmatrix} 1/3 & \sqrt{1/18} & \sqrt{1/18} & 1/3 \\ \sqrt{1/18} & 1/6 & 1/6 & \sqrt{1/18} \\ \sqrt{1/18} & 1/6 & 1/6 & \sqrt{1/18} \\ 1/3 & \sqrt{1/18} & \sqrt{1/18} & 1/3 \end{bmatrix},$$

and whose corresponding classical correlated distribution is

$$p = \begin{bmatrix} 1/3 & 1/6 \\ 1/6 & 1/3 \end{bmatrix},$$

which is easily verified to be a classical correlated equilibrium.

However, ρ is not a quantum Nash equilibrium. Define a unitary matrix

$$G = \begin{bmatrix} \sqrt{2/3} & \sqrt{1/3} \\ \sqrt{1/3} & -\sqrt{2/3} \end{bmatrix}.$$

Consider

$$\rho' = (G \otimes I)\rho(G \otimes I) = \begin{bmatrix} 1/2 & \sqrt{2}/3 & 0 & -1/6 \\ \sqrt{2}/3 & 4/9 & 0 & -\sqrt{2}/9 \\ 0 & 0 & 0 & 0 \\ -1/6 & -\sqrt{2}/9 & 0 & 1/18 \end{bmatrix}.$$

It is easily seen that ρ' has higher expected utility value for player 1, actually

$$\mu_1(\rho') = 206, \qquad \mu_1(\rho) = 201.$$

C.2 Proof of the Second Statement

Let $\rho = |\psi\rangle\langle\psi| = \sum_{a,b} \sqrt{p(a)p(b)}|a\rangle\langle b|$. Then

$$\begin{aligned} \mu_i(\rho) &= \sum_s \langle s|\rho|s\rangle u_i(s) \\ &= \sum_s \langle s| \sum_{a,b} \sqrt{p(a)p(b)}|a\rangle\langle b||s\rangle u_i(s) \\ &= \sum_s p(s)u_i(s) \\ &= \sum_{s_i} p_i(s_i) \sum_{s_{-i}} p_{-i}(s_{-i})u_i(s_i, s_{-i}) \\ &= \sum_{s_i : p_i(s_i) > 0} p_i(s_i) \sum_{s_{-i}} p_{-i}(s_{-i})u_i(s_i, s_{-i}) \end{aligned}$$

Now assume that Player i applies an admissible super-operator Φ_i on ρ:

$$\Phi_i(\rho) = \sum_{j=1}^{k} (A_{ij} \otimes I_{-i})\rho(A_{ij}^* \otimes I_{-i})$$

where $\sum_{j=1}^{k} A_{ij}^* A_{ij} = I_i$.
Let $\bar{s}_i$ be a strategy *s.t.* $p_i(\bar{s}_i) > 0$. Then by the definition of Nash equilibrium, we have

$$\sum_{s_i} p_{-i}(s_{-i}) u_i(s_i s_{-i}) \leq \sum_{s_i} p_{-i}(s_{-i}) u_i(\bar{s}_i s_{-i}), \tag{18}$$

for any s_i.

$$\begin{aligned}
\mu_i(\Phi_i(\rho)) &= \sum_s \langle s|\Phi_i(\rho)|s\rangle u_i(s) \\
&= \sum_s \langle s| \sum_{j=1}^{k} (A_{ij} \otimes I_{-i}) \rho (A_{ij}^* \otimes I_{-i}) |s\rangle u_i(s) \\
&= \sum_s \langle s| \sum_{j=1}^{k} (A_{ij} \otimes I_{-i}) \sum_{a,b} \sqrt{p(a)p(b)} |a\rangle\langle b| (A_{ij}^* \otimes I_{-i}) |s\rangle u_i(s) \\
&= \sum_{s,a,b,j} \sqrt{p(a)p(b)} \langle s|(A_{ij} \otimes I_{-i})|a\rangle\langle b|(A_{ij}^* \otimes I_{-i})|s\rangle u_i(s) \\
&= \sum_{s,a,b,j} \sqrt{p_i(a_i)p_i(b_i)} \sqrt{p_{-i}(a_{-i})p_{-i}(b_{-i})} \langle s_i|A_{ij}|a_i\rangle\langle s_{-i}|a_{-i}\rangle\langle b_i|A_{ij}^*|s_i\rangle\langle b_{-i}|s_{-i}\rangle u_i(s) \\
&= \sum_{s_i,s_{-i},a_i,b_i,j} \sqrt{p_i(a_i)p_i(b_i)} \langle s_i|A_{ij}|a_i\rangle\langle b_i|A_{ij}^*|s_i\rangle p_{-i}(s_{-i}) u_i(s_i, s_{-i}) \\
&= \sum_{s_i,s_{-i},a_i,b_i,j:p_i(a_i)>0,p_i(b_i)>0} \sqrt{p_i(a_i)p_i(b_i)} \langle s_i|A_{ij}|a_i\rangle\langle b_i|A_{ij}^*|s_i\rangle p_{-i}(s_{-i}) u_i(s_i, s_{-i}) \\
&= \sum_{s_i,a_i,b_i,j:p_i(a_i)>0,p_i(b_i)>0} \sqrt{p_i(a_i)p_i(b_i)} \langle s_i|A_{ij}|a_i\rangle\langle b_i|A_{ij}^*|s_i\rangle \sum_{s_{-i}} p_{-i}(s_{-i}) u_i(s_i, s_{-i}) \\
&\leq \sum_{s_i,a_i,b_i,j:p_i(a_i)>0,p_i(b_i)>0} \sqrt{p_i(a_i)p_i(b_i)} \langle s_i|A_{ij}|a_i\rangle\langle b_i|A_{ij}^*|s_i\rangle \sum_{s_{-i}} p_{-i}(s_{-i}) u_i(a_i, s_{-i})
\end{aligned}$$

$$\begin{aligned}
&= \sum_{s_i,a_i,b_i,j:p_i(a_i)>0,p_i(b_i)>0} \sqrt{p_i(a_i)p_i(b_i)} \langle b_i|A_{ij}^*|s_i\rangle\langle s_i|A_{ij}|a_i\rangle \sum_{s_{-i}} p_{-i}(s_{-i}) u_i(a_i, s_{-i}) \\
&= \sum_{a_i,b_i,j:p_i(a_i)>0,p_i(b_i)>0} \sqrt{p_i(a_i)p_i(b_i)} \langle b_i|A_{ij}^* A_{ij}|a_i\rangle \sum_{s_{-i}} p_{-i}(s_{-i}) u_i(a_i, s_{-i}) \\
&= \sum_{a_i,b_i:p_i(a_i)>0,p_i(b_i)>0} \sqrt{p_i(a_i)p_i(b_i)} \langle b_i|a_i\rangle \sum_{s_{-i}} p_{-i}(s_{-i}) u_i(a_i, s_{-i}) \\
&= \sum_{\bar{s}_i:p_i(\bar{s}_i)>0} p_i(\bar{s}_i) \sum_{s_{-i}} p_{-i}(s_{-i}) u_i(\bar{s}_i, s_{-i}) \\
&= \mu_i(\rho)
\end{aligned}$$

This completes the proof of Theorem 3.4.

From the above proof, one can see that if $supp(p_i) = S_i$, then the only inequality becomes the equality. We thus obtain the following fact.

Corollary C.1 *If p is a classical Nash equilibrium and $supp(p_i) = S_i$, then $|\psi\rangle = \sum_s \sqrt{p(s)}|s\rangle$ is a quantum Nash equilibrium, and any quantum operation by Player i does not change his/her utility value.*

D Examples in Theorem 3.5

Define the utility matrices of both Player 1 and Player 2 to be:

$$u_1 = u_2 = u = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Note that since u is symmetric, so is the game. Below we will show a couple of examples where p_ρ is a classical (sometimes correlated) Nash equilibrium but ρ itself is not a quantum (correlated) Nash equilibrium.

Example 1: a mixed product state

Suppose the initial state is

$$\rho = \frac{1}{2}\begin{bmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & \sin^2(\theta) \end{bmatrix} \otimes |0\rangle\langle 0| + \frac{1}{2}\begin{bmatrix} \sin^2(\theta) & -\cos(\theta)\sin(\theta) \\ -\cos(\theta)\sin(\theta) & \cos^2(\theta) \end{bmatrix} \otimes |1\rangle\langle 1| \tag{19}$$

$$= \begin{bmatrix} \cos^2(\theta)/2 & & \cos(\theta)\sin(\theta)/2 & \\ & \sin^2(\theta)/2 & & -\cos(\theta)\sin(\theta)/2 \\ \cos(\theta)\sin(\theta)/2 & & \sin^2(\theta)/2 & \\ & -\cos(\theta)\sin(\theta)/2 & & \cos^2(\theta)/2 \end{bmatrix} \tag{20}$$

Take the diagonal elements to form a classical correlated distribution

$$p = \begin{bmatrix} \cos^2(\theta)/2 & \sin^2(\theta)/2 \\ \sin^2(\theta)/2 & \cos^2(\theta)/2 \end{bmatrix},$$

which is easily verified to be a classical correlated equilibrium if $\cos^2(\theta) \geq 1/2$.

However, ρ is not a quantum Nash equilibrium. Define a unitary matrix

$$G = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}.$$

Consider

$$\rho' = (G \otimes I)\rho(G \otimes I) = \begin{bmatrix} 1/2 & & & \\ & 0 & & \\ & & 0 & \\ & & & 1/2 \end{bmatrix}$$

It is easily seen that ρ' has higher expected utility value for player 1, actually

$$\mu_1(\rho') = 2, \qquad \mu_1(\rho) = 1 + \cos^2(\theta).$$

Example 2: an entangled pure state

Consider

$$\rho = \frac{1}{2}\begin{bmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta) & \cos(\theta)\sin(\theta) & -\cos^2(\theta) \\ \cos(\theta)\sin(\theta) & \sin^2(\theta) & \sin^2(\theta) & -\cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & \sin^2(\theta) & \sin^2(\theta) & -\cos(\theta)\sin(\theta) \\ -\cos^2(\theta) & -\cos(\theta)\sin(\theta) & -\cos(\theta)\sin(\theta) & \cos^2(\theta) \end{bmatrix}$$

Since the diagonal entries are the same as those in Eq. (19), the induced classical distribution is also the same as before, which is a classical correlated equilibrium. Again, ρ is not a quantum Nash equilibrium since

$$\rho' = (G \otimes I)\rho(G \otimes I) = \begin{bmatrix} 1/2 & & & 1/2 \\ & 0 & & \\ & & 0 & \\ 1/2 & & & 1/2 \end{bmatrix}$$

and it is easy to see that $\mu_1(\rho') = 2$.

Example 3: (uncorrelated) Nash equilibrium

Suppose

$$\rho = \begin{bmatrix} 1/4 & 1/4 & 1/4 & -1/4 \\ 1/4 & 1/4 & 1/4 & -1/4 \\ 1/4 & 1/4 & 1/4 & -1/4 \\ -1/4 & -1/4 & -1/4 & 1/4 \end{bmatrix}$$

The induced classical distribution is now

$$p = \begin{bmatrix} 1/4 & 1/4 \\ 1/4 & 1/4 \end{bmatrix}.$$

It is easy to check that this is a classical correlated equilibrium. Consider

$$\rho' = (H \otimes I)\rho(H \otimes I) = \begin{bmatrix} 1/2 & & & 1/2 \\ & 0 & & \\ & & 0 & \\ 1/2 & & & 1/2 \end{bmatrix}$$

where H is the Hadamard matrix. Here $\mu_1(\rho') = 2 > \mu_1(\rho)$. Therefore ρ is not a quantum Nash equilibrium.

E Examples for Theorem 3.6

Define the utility matrices of both Player 1 and Player 2 to be:

$$u_1 = u_2 = u = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \tag{21}$$

Consider the classical correlated distribution

$$p = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}, \tag{22}$$

It is easy to check that this is a classical correlated equilibrium.

For any quantum state ρ with $\rho_{ss} = p(s)$, the expected utility value for player 1 is given by $\mu_1(\rho') = 2$. It is impossible to have any density operator ρ' with $\mu_1(\rho') > 2$. It is easy to see that the expected utility value is maximized so ρ is a quantum Nash equilibrium.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de