科技部補助

大專學生研究計畫研究成果報告

計畫名稱：	Analyzing Quantum Cryptography and Communication based on Quantum Game Theory 量子賽局理論應用於量子密鑰傳輸之分析

報告類別：成果報告
執行計畫學生：蘇磐洋
學生計畫編號：MOST 110-2813-C-002-051-E
研究期間：110年07月01日至111年02月28日止，計8個月
指導教授：鄭皓中

處理方式：本計畫可公開查詢

執行單位：國立臺灣大學電信工程學研究所

中華民國　111年03月28日

Analyzing Quantum Cryptography and Communication based on Quantum Game Theory

— A Game-Theoretic Approach to Achieve Quantum Advantages

Pan-Yang Su[1]

[1]Department of Electrical Engineering, National Taiwan University, Taiwan

(Supervised under Prof. Hao-Chung Cheng at the Department of Electrical Engineering, National Taiwan University)

CONTENTS

I Introduction 3

II Related Works 4

III Quantum Game without Entanglement and Classical Game 6

III-A Two-Player Two-Strategy Game 6

III-B Two-Player Multi-Strategy Game 7

III-C Multi-Player Multi-Strategy Game 8

IV Quantum Two-Player Two-Strategy Game 8

IV-A $\phi = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ 8

IV-B Stability when $\phi = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ 11

IV-C $\phi = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$ 13

IV-D $\phi = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$ 13

IV-E $\phi = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$ 14

V Quantum Multi-Player Two-Strategy Game 14

V-A $\phi = \frac{|00...0\rangle+|11...1\rangle}{\sqrt{2}}$ 14

V-B $\phi = \frac{a+\bar{a}}{\sqrt{2}}$ 15

VI Quantum Two-Player Multi-Strategy Game 15

VII Future Works 16
VII-A Graph States 16
VII-B Stability 17
VII-C Multi-Player Multi-Strategy Game 17
VII-D Quantum Communication and Cryptography Protocols 17

VIII Conclusions 17

References 18

Abstract

Quantum game theory utilizes the power of quantum computation: entanglement and superposition. In particular, without entanglement, quantum games are identical to classical games. However, there are no general rules for quantum advantage in a quantum game. Therefore, we aim to explore sufficient conditions for quantum advantage in this paper. In particular, we identify two aspects of quantum advantage: utility and stability. The first aspect means that quantum strategies can lead to outcomes unobtainable for classical ones. The second aspect implies that the players will naturally fall into the quantum Nash equilibrium through gradient-based learning. Thus, this paper provides more insights into quantum advantage and non-local games.

The overview of this report is given below.

1) **Sec. I:** We give an introduction to quantum game theory and its relationship with quantum communication and cryptography.
2) **Sec. II:** We review some of the related works regarding non-local games, quantum game theory, and their applications.
3) **Sec. III:** We give a mathematical description of the relationship between quantum games without entanglement and classical games.
4) **Sec. IV:** We provide a sufficient condition for quantum advantage in a two-player two-strategy game and discuss the stability issue of the Nash equilibrium.
5) **Sec. V:** We generalize the model of a two-player two-strategy game to a multi-player two-strategy game.
6) **Sec. VI:** We generalize the model of a two-player two-strategy game to a two-player multi-strategy game.
7) **Sec. VII:** We list some future works of the theoretical research and applications of quantum game theory.
8) **Sec. VIII:** We summarize the contributions of this research and draw our conclusions.

Index Terms

game theory, quantum advantage, entanglement, quantum communication, quantum key distribution

I. Introduction

With the advent of the Noisy Intermediate-Scale Quantum (NISQ) era [1], many countries are striving to demonstrate quantum advantages. A critical part of quantum computation and quantum information is quantum communication. By now, plenty of quantum cryptography and communication protocols have been proposed. However, how to quantitatively analyze quantum communication systems is still a huge problem. No general benchmark exists for quantum cryptography and communication protocols, making it difficult to compare them or demonstrate quantum advantages. In classical communication, researchers adopt game theory to compare different systems widely. Therefore, it is natural to use game theory in the quantum domain.

Nonetheless, there are two challenges for using quantum game theory to analyze quantum communication networks. First, the current quantum protocols are cooperative rather than competitive. On the other hand, game theory is most suitable for investigating competitive scenarios. Therefore, it is better to view the protocols from an optimization viewpoint, where the goal is to optimize an objective function, instead of the game-theoretic analysis, where each player has different objectives. Second, large-scale quantum algorithms are hard to analyze inherently. Thus, before a comprehensive treatment of quantum game theory, it is more desirable to have a deeper understanding of a simple yet profound quantum game: non-local games.

Non-local games are widely utilized by researchers to compare classical and quantum resources because the game structure can quantify quantum advantage. For example, we often use the CHSH game to demonstrate the separation between classical theories and quantum ones [2]. The CHSH inequality is a Bell-type inequality, and we can use the CHSH game to prove Bell's theorem experimentally [3]. However, past researchers only examined non-local games from a quantum viewpoint instead of a game-theoretic one. In this research, we aim to approach non-local games from a game-theoretic point of view.

The main contributions of this research are summarized as follows.

1) We identify two aspects of quantum advantage: utility and stability. To the best of our knowledge, we are the first to point out the importance of stability in quantum games.
2) We provide a sufficient condition for utility superiority under a general multi-player two-strategy game.
3) We give a method to identify stability under a general multi-player two-strategy game. This relates gradient-based learning in games and control theory.

The rest of this report is organized as follows. In Sec. II, we review some of the related works. In Sec. III, we argue that quantum games without entanglement are identical to classical games. In Sec. IV, we provide the sufficient condition for quantum advantage in a two-player two-strategy game and discuss the stability issue of the Nash equilibrium. In Sec. V and Sec. VI, we generalize the model to the multi-player two-strategy game and the two-player multi-strategy game, respectively. After that, we give some future works in Sec. VII. Finally, we draw our conclusions in Sec. VIII.

II. Related Works

Clauser *et al.* propose the CHSH game, the most renowned non-local game that demonstrates quantum advantage [2]. When no communication is allowed, the optimal winning probability in the CHSH game using classical strategies is 75%, but 85% when allowing entanglement. The separation between classical and quantum game theory is the different resources allowed, just like the difference between classical and quantum communication.

Eisert *et al.* lay the foundations of quantum game theory [4]. Though they only discuss the prisoner's dilemma, a symmetric two-player game, it identifies the essential elements in a quantum game. As Fig. 1 has shown, a quantum game consists of an initial state ($\hat{J}\,|C\rangle$) for each player, a method each player can manipulate its state ($\hat{U}_A$and $\hat{U}_B$), and a measuring device.

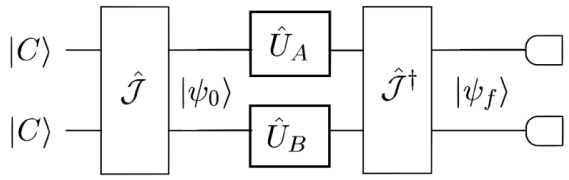

Fig. 1. The setup of a two-player quantum game from [4]

This model is generalized in [5] and [6]. Benjamin *et al.* generalizes the two-player two-strategy model to multi-player quantum games [5]. Though the approach in [5] is similar to that in [4], as can be seen in Fig. 2, it gives us an interpretation of this model. The construction of the game can be viewed as the flow of information, clearly relating quantum game theory to quantum information.

Bolonek-Lasoń *et al.* generalizes the two-player two-strategy model to two-player multi-strategy quantum games [6]. To make its model generalizable, they introduce a lot of parameters to control the degree of entanglement between the two players' strategies. For example, $\hat{J}$ in [4] is generalized to the equation (30) in [6], which is quite complicated.

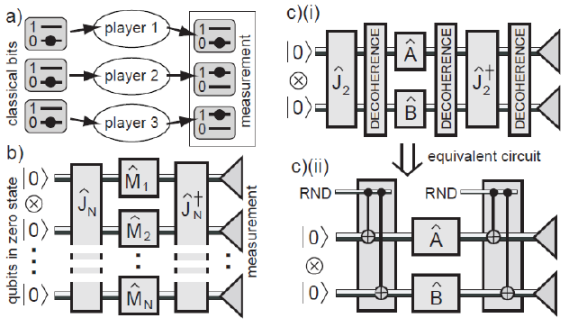

Fig. 2. The setup of a multi-player quantum game from [5]

Solmeyer *et al.* discusses two-player Bayesian quantum games [7]. One player has two types. Thus, we can view the whole game as randomization of two games. The two payoff matrices for the two games are shown in Fig. 3. The upper game is symmetric, while the lower one is not. It seems that whether the game is symmetric or not does not affect the circuit formulation much.

$A \vert B_1$	$\vert 0\rangle\ (C)$	$\vert 1\rangle\ (D)$
$\vert 0\rangle\ (C)$	$(11, 9)$	$(1, 10)$
$\vert 1\rangle\ (D)$	$(10, 1)$	$(6, 6)$

$A \vert B_2$	$\vert 0\rangle\ (C)$	$\vert 1\rangle\ (D)$
$\vert 0\rangle\ (C)$	$(11, 9)$	$(1, 6)$
$\vert 1\rangle\ (D)$	$(10, 1)$	$(6, 0)$

Fig. 3. The payoff matrices of a Bayesian quantum game from [7]

Aoki *et al.* discusses repeated quantum games [8]. Moreover, [8] explores some properties of infinitely repeated quantum games, whose properties are quite different from stage games or finitely repeated quantum games. However, [8] only analyzes the repeated prisoner's dilemma in a particular case. How to use the techniques in [8] in other areas deserves more future research.

Besides the theoretical part of quantum game theory, the followings are examples of game theory in real applications.

Zhang *et al.* discusses quantum gambling based on the concept of Nash equilibrium [9]. It discusses a mechanism for gambling that does not require a trusted third party and that guarantees the existence of a Nash equilibrium. The benefit of not requiring a trusted third

party makes it more feasible for fair gambling. The existence of a Nash equilibrium makes the players' strategies more predictable.

In [10], game theory is used to analyze the behaviors of the sender, the receiver, and the eavesdropper in a BB84 communication system. The result is a Nash equilibrium with each player randomly choosing between the two bases. Though [10] uses the concept of game theory, in particular Nash equilibrium, to analyze a quantum communication system, its game model is classical without a quantum strategy. Thus, [10] gives us little insight into quantum game theory but a simple attempt to use game theory in the field of quantum communication.

III. Quantum Game without Entanglement and Classical Game

In this section, we will demonstrate that a quantum game without entanglement is exactly the same as a classical static game with discrete strategy sets. That is, superposition alone can not provide quantum advantage. Note that different settings may lead to different results. We use the framework in [4], which is the most widely used structure of a quantum game.

A. Two-Player Two-Strategy Game

First, we consider a two-player two-strategy game. Each player has two strategies: 0 or 1. To turn it into a quantum game, we can transform the strategy to $|0\rangle$ and $|1\rangle$. More generally, we can follow the paradigm in [4], but we consider the case without entanglement. So, we can get the following.

$$\left|\psi_f\right\rangle = (U_A \otimes U_B)\,|\psi_i\rangle \tag{1}$$

$|\psi_i\rangle$ is the initial two-qubit state, which is known to both players. U_A and U_B, unitary matrices, are the strategies of the players. $\left|\psi_f\right\rangle$ is the final two-qubit state, which will then be measured to determine the payoffs of both players.

TABLE I

Two-Player Two-Strategy Game

Payoff		B	
		1	2
A	1	$R_A(00), R_B(00)$	$R_A(01), R_B(01)$
	2	$R_A(10), R_B(10)$	$R_A(11), R_B(11)$

The payoffs are given in Table. I. Note that we only consider the first player Alice's payoff to simplify the calculations. Alice's payoff can be expressed as follows.

$$\begin{aligned} R_A = {} & R_A(00)P(00) + R_A(01)P(01) \\ & + R_A(10)P(10) + R_A(11)P(11) \end{aligned} \tag{2}$$

$P(ab)$, where $a = 0, 1$ and $b = 0, 1$, is $\left|\left\langle ab|\psi_f\right\rangle\right|^2$. If we take $|\psi_i\rangle$ as $|00\rangle$, $P(ab)$ can be written as follows. Note that the selection of $|\psi_i\rangle$ does not affect the calculations as long as it is not entangled.

$$\begin{aligned} P(ab) &= \left|\left\langle ab|\psi_f\right\rangle\right|^2 \\ &= |(\langle a| \otimes \langle b|)(U_A \otimes U_B)(|0\rangle \otimes |0\rangle|^2 \\ &= |(\langle a| U_A |0\rangle)(\langle b| U_B |0\rangle)|^2 \\ &= \left|U_{A_{a0}}\right|^2 \left|U_{B_{b0}}\right|^2 \end{aligned} \tag{3}$$

Thus, we can view this expression as a mixed strategy with Alice plays 0 with probability $U^2_{A_{00}}$ and 1 with probability $U^2_{A_{10}}$, and Bob plays 0 with probability $U^2_{B_{00}}$ and 1 with probability $U^2_{B_{10}}$. Also, since U_A and U_B are unitary matrices, $\left|U_{A_{00}}\right|^2 + \left|U_{A_{10}}\right|^2 = 1$ and $\left|U_{B_{00}}\right|^2 + \left|U_{B_{10}}\right|^2 = 1$. Thus, the expression is a valid probability distribution. Therefore, every quantum strategy without entanglement in a two-player two-strategy game can be converted to a mixed strategy, and vice versa.

Note that while we only consider each player applying a unitary matrix, each player can also apply different matrices according to a probability distribution. This is the quantum version of mixed strategies. However, the solution space of this kind of strategy will still be the same as that in the classical mixed strategies.

B. Two-Player Multi-Strategy Game

Now, we consider a two-player multi-strategy game. Without loss of generality, we assume that Alice has 2^m strategies and Bob has 2^n strategies. Then, we can write down $P(ab)$, where $a = 0, 1, ..., 2^m - 1$ and $b = 0, 1, ..., 2^n - 1$, as follows.

$$\begin{aligned} P(ab) &= \left|\left\langle ab|\psi_f\right\rangle\right|^2 \\ &= \left|(\langle a| \otimes \langle b|)(U_A \otimes U_B)(|0\rangle^{\otimes 2^m} \otimes |0\rangle^{\otimes 2^n}\right|^2 \\ &= \left|(\langle a| U_A |0\rangle^{\otimes 2^m})(\langle b| U_B |0\rangle^{\otimes 2^n})\right|^2 \\ &= \left|U_{A_{a0}}\right|^2 \left|U_{B_{b0}}\right|^2 \end{aligned} \tag{4}$$

Therefore, the result is the same as that in the two-player two-strategy game. Every quantum strategy without entanglement in a two-player multi-strategy game can be converted to a mixed strategy, and vice versa.

C. Multi-Player Multi-Strategy Game

Finally, we consider a multi-player multi-strategy game. Without loss of generality, we assume that there are n players and each player i, $i = 1, 2, ..., n$, has 2^{m_i} strategies. Then, we can write down $P(a_1 a_2 ... a_n)$, where $a_i = 0, 1, ..., 2^{m_i} - 1$, as follows.

$$\begin{aligned} P(a_1 a_2 ... a_n) &= \left|\left\langle a_1 a_2 ... a_n \middle| \psi_f \right\rangle\right|^2 \\ &= \left| (\prod_{i=1}^{n} \otimes \langle a_i|)(\prod_{i=1}^{n} \otimes U_i)(\prod_{i=1}^{n} \otimes \langle 0|^{2^{m_i}}) \right|^2 \\ &= \left| \prod_{i=1}^{n} \langle a_i| \, U_i \, |0\rangle^{\otimes 2^{m_i}} \right|^2 \\ &= \prod_{i=1}^{n} \left| U_{i_{a_i 0}} \right|^2 \end{aligned} \tag{5}$$

Therefore, the result is the same as that in the two-player multi-strategy game. Every quantum strategy without entanglement in a multi-player multi-strategy game can be converted to a mixed strategy, and vice versa.

IV. Quantum Two-Player Two-Strategy Game

In this section, we first analyze the utility and stability issues of a Nash equilibrium under a particular initial state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Then, we analyze the quantum Nash equilibria using different Bell states as initial states. Although different initial states may lead to different Nash equilibria, they all have similar structures. Thus, we can say that the resulting Nash equilibria are the same up to some unitary transformations. We will demonstrate this result in more detail in the next section when considering multiple players, so we omit some details in this section.

A. $\phi = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$

In this subsection, we will prove that $P(00) = P(11)$ and $P(01) = P(10)$.

First, note that the initial state is $\rho_{AB} = |\phi\rangle\langle\phi|$, where $\phi = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Then we have the following, where $\langle A, B\rangle_F$ denotes the Frobenius inner product of A and B.

$$\begin{aligned}
&\mathrm{Tr}[\rho_{AB}\Pi_A \otimes \Pi_B] \\
&= \mathrm{Tr}\left[\rho_{AB}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \\
&= \frac{1}{2}(ae + bf + cg + dh) \\
&= \frac{1}{2}\langle \Pi_A^\star, \Pi_B\rangle_F
\end{aligned} \tag{6}$$

Then, we parameterize Π_A^0 and Π_B^0. We parameterize $\Pi_A^0 = |u\rangle\langle u|$, where $|u\rangle = \cos\frac{\theta_A}{2}|0\rangle + \sin\frac{\theta_A}{2}e^{i\phi_A}|1\rangle$. We parameterize $\Pi_B^0 = |w\rangle\langle w|$, where $|w\rangle = \cos\frac{\theta_B}{2}|0\rangle + \sin\frac{\theta_B}{2}e^{i\phi_B}|1\rangle$. Therefore, we have the following.

$$\Pi_A^0 = \begin{pmatrix} \cos^2\frac{\theta_A}{2} & \cos\frac{\theta_A}{2}\sin\frac{\theta_A}{2}e^{-i\phi_A} \\ \cos\frac{\theta_A}{2}\sin\frac{\theta_A}{2}e^{i\phi_A} & \sin^2\frac{\theta_A}{2} \end{pmatrix} \tag{7}$$

$$\Pi_B^0 = \begin{pmatrix} \cos^2\frac{\theta_B}{2} & \cos\frac{\theta_B}{2}\sin\frac{\theta_B}{2}e^{-i\phi_B} \\ \cos\frac{\theta_B}{2}\sin\frac{\theta_B}{2}e^{i\phi_B} & \sin^2\frac{\theta_B}{2} \end{pmatrix} \tag{8}$$

So, we can get the probability distribution over all the outcomes as the following.

$$P(00) = \frac{1}{2}\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F \tag{9}$$

$$P(01) = \frac{1}{2}\langle \Pi_A^{0\star}, I - \Pi_B^0\rangle_F \tag{10}$$

$$P(10) = \frac{1}{2}\langle I - \Pi_A^{0\star}, \Pi_B^0\rangle_F \tag{11}$$

$$P(11) = \frac{1}{2}\langle I - \Pi_A^{0\star}, I - \Pi_B^0\rangle_F \tag{12}$$

Based on $\mathrm{Tr}\left[\Pi_A^0\right] = \mathrm{Tr}\left[\Pi_B^0\right] = 1$, we can get the following equations.

$$\langle I, \Pi_B^0\rangle_F + \langle \Pi_A^{0\star}, I\rangle_F = 2 \tag{13}$$

$$\langle I, \Pi_B^0\rangle_F = \langle \Pi_A^{0\star}, I\rangle_F \tag{14}$$

Therefore, the solution space is restricted to $P(00) = P(11)$ and $P(01) = P(10)$.

Then, we will solve the Nash equilibria.

$$\begin{aligned}
R_A &= \frac{R_A(01) + R_A(10)}{2}\langle \Pi_A^{0\star}, I - \Pi_B^0\rangle_F \\
&\quad + \frac{R_A(00) + R_A(11)}{2}\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F \\
&= \frac{R_A(00) + R_A(11) - R_A(01) - R_A(10)}{2}\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F \\
&\quad + \frac{R_A(01) + R_A(10)}{2}
\end{aligned} \tag{15}$$

$$\begin{aligned} R_B &= \frac{R_B(01)+R_B(10)}{2}\langle \Pi_A^{0\star}, I-\Pi_B^0\rangle_F \\ &+ \frac{R_B(00)+R_B(11)}{2}\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F \\ &= \frac{R_B(00)+R_B(11)-R_B(01)-R_B(10)}{2}\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F \\ &+ \frac{R_B(01)+R_B(10)}{2} \end{aligned} \tag{16}$$

Thus, solving the Nash equilibria of the game corresponds to solving the Nash equilibria of $\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F$. Now, we write down $\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F$ explicitly.

$$\begin{aligned} &\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F \\ &= \cos^2\frac{\theta_A}{2}\cos^2\frac{\theta_B}{2} + \sin^2\frac{\theta_A}{2}\sin^2\frac{\theta_B}{2} \\ &+ 2\cos\frac{\theta_A}{2}\sin\frac{\theta_A}{2}\cos\frac{\theta_B}{2}\sin\frac{\theta_B}{2}\cos(\phi_A+\phi_B) \end{aligned} \tag{17}$$

Next, by differentiating $\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F$ with respect to different variables, we have the following.

$$\begin{aligned} &\frac{\partial\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F}{\partial\theta_A} \\ &= \cos\frac{\theta_A}{2}\sin\frac{\theta_A}{2}(\sin^2\frac{\theta_B}{2}-\cos^2\frac{\theta_B}{2}) \\ &+ (\cos^2\frac{\theta_A}{2}-\sin^2\frac{\theta_A}{2})\cos\frac{\theta_B}{2}\sin\frac{\theta_B}{2}\cos(\phi_A+\phi_B) \\ &= -\frac{1}{2}\sin\theta_A\cos\theta_B + \frac{1}{2}\cos\theta_A\sin\theta_B\cos(\phi_A+\phi_B) \end{aligned} \tag{18}$$

$$\begin{aligned} &\frac{\partial\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F}{\partial\phi_A} \\ &= -2\cos\frac{\theta_A}{2}\sin\frac{\theta_A}{2}\cos\frac{\theta_B}{2}\sin\frac{\theta_B}{2}\sin(\phi_A+\phi_B) \\ &= -\frac{1}{2}\sin\theta_A\sin\theta_B\sin(\phi_A+\phi_B) \end{aligned} \tag{19}$$

$$\begin{aligned} &\frac{\partial\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F}{\partial\theta_B} \\ &= -\frac{1}{2}\cos\theta_A\sin\theta_B + \frac{1}{2}\sin\theta_A\cos\theta_B\cos(\phi_A+\phi_B) \end{aligned} \tag{20}$$

$$\begin{aligned} &\frac{\partial\langle \Pi_A^{0\star}, \Pi_B^0\rangle_F}{\partial\phi_B} \\ &= -\frac{1}{2}\sin\theta_A\sin\theta_B\sin(\phi_A+\phi_B) \end{aligned} \tag{21}$$

The above equations should all equal to 0, so we have three situations: $\sin\theta_A = 0$, $\sin\theta_B = 0$, or $\sin\phi_C = 0$, where $\phi_C = \phi_A + \phi_B$.

When $\sin\theta_A = 0$, we have $\sin\theta_B = 0$ and ϕ_C can be any number. When $\sin\theta_B = 0$, we have $\sin\theta_A = 0$ and ϕ_C can be any number. Therefore, the two situations become the same one.

From the analysis, we find out that $R(00)+R(11) \geq R(01)+R(10)$ is a sufficient condition for $P(00) = P(11) = 0.5$ being a Nash equilibrium. As such, we can break the prisoner's dilemma if $R+P \geq S+T$, where we have used the definitions in Fig. 4. This result is similar to that in [11] in that the payoff matrix determines whether quantum strategies are better than classical ones.

Canonical PD payoff matrix

Blue \ Red	Cooperate	Defect
Cooperate	R, R	T, S
Defect	S, T	P, P

and to be a prisoner's dilemma game in the strong sense, the following condition must hold for the payoffs:

$$T > R > P > S$$

Fig. 4. An example of canonical prisoner's dilemma from [12]

B. *Stability when* $\phi = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$

According to [13], define $\omega(x) = (D_1 f_1(x), D_2 f_2(x))$ to be the vector of player derivatives of their own payoff functions with respect to their own choice variables, we have the following.

Definition 1 (LASE)**.** *A point $x \in X$ is a locally asymptotically stable equilibrium of the continuous time dynamics $\dot{x} = \omega(x)$ if $\omega(x) = 0$ and $Re(\lambda) > 0$ for all $\lambda \in spec(D\omega(x))$.*

Suppose $\phi = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, we have the following, where $R_{AT} = \frac{R_A(00)+R_A(11)-R_A(01)-R_A(10)}{2}$

$$\begin{aligned} &D_{\theta_A} f_1(x) \\ &= -(\frac{1}{2}\sin\theta_A\cos\theta_B + \frac{1}{2}\cos\theta_A\sin\theta_B\cos(\phi_A+\phi_B))R_{AT} \end{aligned} \tag{22}$$

$$\begin{aligned} &D^2_{\theta_A} f_1(x) \\ &= (-\frac{1}{2}\cos\theta_A\cos\theta_B + \frac{1}{2}\sin\theta_A\sin\theta_B\cos(\phi_A+\phi_B))R_{AT} \end{aligned} \tag{23}$$

$$\begin{aligned} &D_{\phi_A} D_{\theta_A} f_1(x) \\ &= \frac{1}{2}\cos\theta_A\sin\theta_B\sin(\phi_A+\phi_B)R_{AT} \end{aligned} \tag{24}$$

$$
\begin{aligned}
&D_{\phi_A} f_1(x) \\
&= -\frac{1}{2} \sin\theta_A \sin\theta_B \sin(\phi_A + \phi_B) R_{AT}
\end{aligned} \tag{25}
$$

$$
\begin{aligned}
&D_{\theta_A} D_{\phi_A} f_1(x) \\
&= -\frac{1}{2} \cos\theta_A \sin\theta_B \sin(\phi_A + \phi_B) R_{AT}
\end{aligned} \tag{26}
$$

$$
\begin{aligned}
&D^2_{\phi_A} f_1(x) \\
&= -\frac{1}{2} \sin\theta_A \sin\theta_B \cos(\phi_A + \phi_B) R_{AT}
\end{aligned} \tag{27}
$$

Also, we have the following Jacobian. If $\sin\theta_A = \sin\theta_B = 0$, $\omega(x) = 0$, and $D\omega(x)$ is the following.

$$
D\omega(x) = \begin{pmatrix} D^2_1 f_1(x) & D_{21} f_1(x) \\ D_{12} f_2(x) & D^2_2 f_2(x) \end{pmatrix} \tag{28}
$$

$$
\begin{aligned}
D^2_1 f_1(x) &= \begin{pmatrix} D^2_{\theta_A} f_1(x) & D_{\phi_A} D_{\theta_A} f_1(x) \\ D_{\theta_A} D_{\phi_A} f_1(x) & D^2_{\phi_A} f_1(x) \end{pmatrix} \\
&= \begin{pmatrix} -\frac{R_{AT} \cos\theta_A \cos\theta_B}{2} & 0 \\ 0 & 0 \end{pmatrix}
\end{aligned} \tag{29}
$$

$$
\begin{aligned}
D_{21} f_1(x) &= \begin{pmatrix} D_{\theta_B} D_{\theta_A} f_1(x) & D_{\phi_B} D_{\theta_A} f_1(x) \\ D_{\theta_B} D_{\phi_A} f_1(x) & D_{\phi_B} D_{\phi_A} f_1(x) \end{pmatrix} \\
&= \begin{pmatrix} -\frac{R_{AT} \cos\theta_A \cos\theta_B \cos\phi_C}{2} & 0 \\ 0 & 0 \end{pmatrix}
\end{aligned} \tag{30}
$$

$$
D_{12} f_2(x) = \begin{pmatrix} -\frac{R_{BT} \cos\theta_A \cos\theta_B \cos\phi_C}{2} & 0 \\ 0 & 0 \end{pmatrix} \tag{31}
$$

$$
D^2_2 f_2(x) = \begin{pmatrix} -\frac{R_{BT} \cos\theta_A \cos\theta_B}{2} & 0 \\ 0 & 0 \end{pmatrix} \tag{32}
$$

We have $\lambda = 0$ corresponding to $(0, 1, 0, 0)^T$ and $(0, 0, 0, 1)^T$. For another λ, we would like to solve $(R_{AT}(a + \cos\phi), 0, R_{BT}(a\cos\phi + 1), 0) = \lambda(a, 0, 1, 0)$. Then, we have $R_{BT}\cos\phi a^2 + (R_{BT} - R_{AT})a + R_{AT}\cos\phi$, and $\lambda'^2 - (R_{AT} + R_{BT})\lambda' + R_{AT}R_{BT}(1 - \cos^2\phi)$, where $\lambda' = -\frac{\cos\theta_A \cos\theta_B}{2}\lambda$. We have $\lambda'_1 + \lambda'_2 = R_{AT} + R_{BT}$, and $\lambda'_1\lambda'_2 = R_{AT}R_{BT}(1 - \cos^2\phi)$, so $\lambda'_1 \geq 0$, and $\lambda'_2 \geq 0$. Thus, to have an LASE, we must have $\cos\theta_A \cos\theta_B = -1$.

C. $\phi = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$

First, note that the initial state is $\rho_{AB} = |\phi\rangle\langle\phi|$, where $\phi = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$. Then we have the following, where $\tilde{\Pi}_B$ is the matrix obtained by rotating each element of Π_B by a half circle with respect to the center. That is $\tilde{\Pi}_B(ij) = \Pi_B(\bar{i}\bar{j})$. Also, using the qubit representation, we have $\tilde{\theta_B} = \pi/2 - \theta_B$ and $\tilde{\phi_B} = -\phi_B$

$$\begin{aligned} &\mathrm{Tr}[\rho_{AB}\Pi_A \otimes \Pi_B] \\ &= \mathrm{Tr}\left[\rho_{AB}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \\ &= \frac{1}{2}(ah + bg + cf + de) \\ &= \frac{1}{2} sum(\Pi_A \circ \tilde{\Pi_B}) \end{aligned} \tag{33}$$

So, we can get the probability distribution over all the outcomes as the following. Thus, $P(00) = P(11)$ and $P(01) = P(10)$.

$$P(00) = \frac{1}{2}(ah + bg + cf + de) \tag{34}$$

$$P(01) = \frac{1}{2}(a(1-h) + bg + cf + d(1-e)) \tag{35}$$

$$P(10) = \frac{1}{2}((1-a)h + bg + cf + (1-d)e) \tag{36}$$

$$P(11) = \frac{1}{2}((1-a)(1-h) + bg + cf + (1-d)(1-e)) \tag{37}$$

Then, we will solve the Nash equilibria.

$$\begin{aligned} R_A = &(R_A(01) + R_A(10))P(01) \\ &+ (R_A(00) + R_A(11))P(00) \end{aligned} \tag{38}$$

$$\begin{aligned} R_B = &(R_B(01) + R_B(10))P(01) \\ &+ (R_B(00) + R_B(11))P(00) \end{aligned} \tag{39}$$

D. $\phi = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$

First, note that the initial state is $\rho_{AB} = |\phi\rangle\langle\phi|$, where $\phi = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$. Then we have the following.

$$\begin{aligned} &\mathrm{Tr}[\rho_{AB}\Pi_A \otimes \Pi_B] \\ &= \mathrm{Tr}\left[\rho_{AB}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \\ &= \frac{1}{2}(ae - bf - cg + dh) \end{aligned} \tag{40}$$

So, we can get the probability distribution over all the outcomes as the following. Thus, $P(00) = P(11)$ and $P(01) = P(10)$.

$$P(00) = \frac{1}{2}(ae - bf - cg + dh) \tag{41}$$

$$P(01) = \frac{1}{2}(a(1-e) - bf - cg + d(1-h)) \tag{42}$$

$$P(10) = \frac{1}{2}((1-a)e - bf - cg + (1-d)h) \tag{43}$$

$$P(11) = \frac{1}{2}((1-a)(1-e) - bf - cg + (1-d)(1-h)) \tag{44}$$

E. $\phi = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$

First, note that the initial state is $\rho_{AB} = |\phi\rangle\langle\phi|$, where $\phi = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$. Then we have the following.

$$\begin{aligned} &\mathrm{Tr}[\rho_{AB}\Pi_A \otimes \Pi_B] \\ &= \mathrm{Tr}\left[\rho_{AB}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} e & f \\ g & h \end{pmatrix}\right] \\ &= \frac{1}{2}(ah - bg - cf + de) \end{aligned} \tag{45}$$

So, we can get the probability distribution over all the outcomes as the following. Thus, $P(00) = P(11)$ and $P(01) = P(10)$.

$$P(00) = \frac{1}{2}(ah - bg - cf + de) \tag{46}$$

$$P(01) = \frac{1}{2}(a(1-h) - bg - cf + d(1-e)) \tag{47}$$

$$P(10) = \frac{1}{2}((1-a)h - bg - cf + (1-d)e) \tag{48}$$

$$P(11) = \frac{1}{2}((1-a)(1-h) - bg - cf + (1-d)(1-e)) \tag{49}$$

V. Quantum Multi-Player Two-Strategy Game

A. $\phi = \frac{|00...0\rangle + |11...1\rangle}{\sqrt{2}}$

We assume there are n players, each with two strategies. First, note that the initial state is $\rho = |\phi\rangle\langle\phi|$, where $\phi = \frac{|00...0\rangle + |11...1\rangle}{\sqrt{2}}$. Then we have the following, where $A \circ B$ denotes the Hadamard product of matrices A and B, and $sum(A)$ denotes the summation of all the elements in A. Note that $\langle A^\star, B\rangle_F = sum(A \circ B)$.

$$\begin{aligned} &\mathrm{Tr}[\rho\Pi_1 \otimes \Pi_2 \otimes ... \otimes \Pi_n] \\ &= \frac{1}{2} sum(\Pi_1 \circ ... \circ \Pi_n) \end{aligned} \tag{50}$$

Now, we would like to show that $P(00...0) = P(11...1) = 0.5$ is a Nash equilibrium no matter the payoff matrix.

Suppose $\cos\theta_j = 1, \sin\theta_j = 0, j \neq i$. Obviously, $\cos\theta_i = 1, \sin\theta_i = 0$ is a best response for player i when $R_i(00...0) + R_i(11...1) \geq R_i(11...0...1) + R_i(00...1...0)$ as demonstrated below.

$$\begin{aligned} R_i &= \frac{\cos^2\frac{\theta_i}{2}}{2} R_i(00...0...0) + \frac{\sin^2\frac{\theta_i}{2}}{2} R_i(11...0...1) \\ &+ \frac{1-\cos^2\frac{\theta_i}{2}}{2} R_i(00...1...0) + \frac{1-\sin^2\frac{\theta_i}{2}}{2} R_i(11...1...1) \\ &= \frac{\cos^2\frac{\theta_i}{2}}{2} (R_i(00...0) + R_i(11...1)) \\ &+ \frac{\sin^2\frac{\theta_i}{2}}{2} (R_i(11...0...1) + R_i(00...1...0)) \end{aligned} \tag{51}$$

Thus, a sufficient condition for $P(00...0) = P(11...1) = 0.5$ being a Nash equilibrium is $R_i(00...0) + R_i(11...1) \geq R_i(11...0...1) + R_i(00...1...0), \forall i$.

B. $\phi = \frac{a+\bar{a}}{\sqrt{2}}$

We assume there are n players, each with two strategies. First, note that the initial state is $\rho = |\phi\rangle\langle\phi|$, where $\phi = \frac{a+\bar{a}}{\sqrt{2}}$. Note that $a + \bar{a} = 2^n + 1$, and ρ is a matrix with only four non-zero elements. That is, $\rho(aa) = \rho(a\bar{a}) = \rho(\bar{a}a) = \rho(\bar{a}\bar{a}) = 1$. Then we have the following, where $A \circ B$ denotes the Hadamard product of matrices A and B, and $sum(A)$ denotes the summation of all the elements in A. Note that $\langle A^\star, B\rangle_F = sum(A \circ B)$.

$$\begin{aligned} &\mathrm{Tr}[\rho\Pi_1 \otimes \Pi_2 \otimes ... \otimes \Pi_n] \\ &= \frac{1}{2} sum(\prod \circ \Pi_i^{\bar{a}_i} \tilde{\Pi}_i^{a_i}) \end{aligned} \tag{52}$$

Note that as long as the initial state is achieved by a sequence of one-qubit unitary transformations of $\phi = \frac{|00...0\rangle + |11...1\rangle}{\sqrt{2}}$, the Nash equilibrium is also a unitary transformation of the original one, i.e., $\cos\theta_i = 0, \forall i$. For example, the Nash equilibrium for $\phi = \frac{|++...+\rangle + |--...-\rangle}{\sqrt{2}}$ is $\Pi_i = |+\rangle\langle+|, \forall i$.

VI. Quantum Two-Player Multi-Strategy Game

We assume there are two players, each with 2^n strategies. First, note that the initial state is $\rho_{AB} = |\phi\rangle\langle\phi|$, where $\phi = \frac{\sum_{x\in\{0,1\}^n} |x\rangle|x\rangle}{2^{n/2}}$. Then we have the following, where $\langle A, B\rangle_F$ denotes the Frobenius inner product of A and B.

$$\begin{aligned} &\mathrm{Tr}[\rho_{AB}\Pi_A \otimes \Pi_B] \\ &= \frac{1}{2^n} \langle \Pi_A^\star, \Pi_B\rangle_F \end{aligned} \tag{53}$$

The strategy of each player is the value of 2^n PVM matrices with the summation of the matrices equal to the identity matrix. That is, we have the following. Note that each matrix is of dimension $2^n \times 2^n$.

$$\sum_{i=0}^{2^n-1} \Pi_A^i = I \tag{54}$$

$$\sum_{i=0}^{2^n-1} \Pi_B^i = I \tag{55}$$

We aim to explore whether $P(xx) = 1/2^n, x = \{0,1\}^n$ is a Nash equilibrium. Assume that for $i = 0, 1, ..., 2^n - 1$, Π_B^i is a matrix with only one non-zero element $\Pi_B^i(ii) = 1$. We want to find out the best response of player A.

Put it more rigorously, we have the following payoff to maximize, and we want to find the sufficient condition for Π_A^i being a matrix with only one non-zero element $\Pi_A^i(ii) = 1$ for $i = 0, 1, ..., 2^n - 1$.

$$R_A = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \Pi_A^i(jj) R_A(ij) \tag{56}$$

Note that we also have $\sum_{j=0}^{2^n-1} \Pi_A^i(jj) = 1$ because these matrices have trace one. Therefore, we have m^2 variables to determine, where $m = 2^n$, and we have $2m - 1$ linearly independent equations corresponding to the m trace constraints and (54). A sufficient condition is $R_A(ii) \geq \sum_{j \neq i} R_A(ij)$ for $i = 0, 1, ..., 2^n - 1$. Note that this condition is similar to the definition of a diagonally dominant matrix.

On the other hand, if we only require $\sum_i R_A(ii) \geq \sum_i \sum_{j \neq i} R_A(ij)$ for $i = 0, 1, ..., 2^n - 1$, we may get a higher payoff without Π_A^i being a matrix with only one non-zero element. We give an example below.

Consider $m = 3$. $\Pi_A^0(00) = \Pi_A^1(11) = 0.8$, $\Pi_A^0(11) = \Pi_A^1(00) = 0.2$, $\Pi_A^0(22) = \Pi_A^1(22) = 0$. Also, Π_A^2 is a matrix with only one non-zero element $\Pi_A^2(22) = 1$. Obviously, as long as $R_A(22)$ is large enough, and $R_A(11)$ or $R_A(22)$ is small enough, we can get a higher payoff.

VII. Future Works

There are some areas for which we have researched, but have not obtained a general result. We provide them as future works listed below.

A. Graph States

Instead of using Bell states and GHZ states as initial states, we would also use graph states or cluster states to account for more general entangled states. The graph states describe a set

of qubits with pair-wise entanglement between some of them. Thus, they are more reasonable initial states in real quantum communication systems, where it is easier to have pair-wise entanglement. We consider a graph $G = (V, E)$, where V is the set of all vertices (players), and E is the set of all edges. The mathematical formulation is given by the following equation from [14], where $U^{(i,j)}$ is the controlled-Z interaction between i and j.

$$\rho = \prod_{(i,j)\in E} U^{(i,j)} \left|+\right\rangle^{\otimes i} \tag{57}$$

B. Stability

As in the two-player two-strategy games, we would like to discuss the stability issue in other types of games. We give a formula for the multi-player two-strategy game in the following.

Suppose $\phi = \frac{|00...0\rangle + |11...1\rangle}{\sqrt{2}}$, we have the following.

$$D_i f_i(x)_{11} = \frac{1}{2} \sum_{a\in\{0,1\}^n} R_i(a) \prod \Pi_{i_{11}}^{\bar{a_j}} (I - \Pi_{i_{11}})^{a_j} \tag{58}$$

C. Multi-Player Multi-Strategy Game

After analyzing the two-player two-strategy game, the multi-player two-strategy game, and the two-player multi-strategy game, a natural extension is the analysis of the multi-player multi-strategy game. This game structure is challenging to analyze due to the enormous number of parameters. However, we believe the exploration of the multi-player multi-strategy game is critical in the research of quantum communication and cryptography protocols.

D. Quantum Communication and Cryptography Protocols

The ultimate goal of this research is to utilize quantum game theory to design or analyze quantum communication and cryptography protocols. Specifically, quantum Internet is a promising use case for it. However, although quantum Internet has sparked a lot of research interest since [15], and some researchers have pointed out the directions for it [16], it is still in its embryonic stage. Therefore, we need to wait for the hardware advancement before applying the theoretical research in real scenarios.

VIII. Conclusions

In this research, we try to provide a comprehensive game-theoretic structure for quantum advantage under different game scenarios. In particular, we have discussed two aspects of

quantum advantage: utility and stability. First, we provide sufficient conditions for demonstrating utility superiority in different game structures. Second, we utilize the concept in control theory and provide a way to calculate stability. On the other hand, there are two future research directions. First, we aim to consider more general game structures and properties. Second, we would like to apply quantum game theory to quantum communication and cryptography protocols, which pave the way for designing the forthcoming quantum Internet.

REFERENCES

[1] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, 2018.

[2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical review letters*, vol. 23, no. 15, p. 880, 1969.

[3] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[4] J. Eisert, M. Wilkens, and M. Lewenstein, "Quantum games and quantum strategies," *Physical Review Letters*, vol. 83, no. 15, p. 3077, 1999.

[5] S. C. Benjamin and P. M. Hayden, "Multiplayer quantum games," *Physical Review A*, vol. 64, no. 3, p. 030301, 2001.

[6] K. Bolonek-Lasoń, "General quantum two-player games, their gate operators, and nash equilibria," *Progress of Theoretical and Experimental Physics*, vol. 2015, no. 2, 2015.

[7] N. Solmeyer, N. M. Linke, C. Figgatt, K. A. Landsman, R. Balu, G. Siopsis, and C. Monroe, "Demonstration of a bayesian quantum game on an ion-trap quantum computer," *Quantum Science and Technology*, vol. 3, no. 4, p. 045002, 2018.

[8] S. Aoki and K. Ikeda, "Repeated quantum games and strategic efficiency," *Available at SSRN 3600788*, 2020.

[9] P. Zhang, X.-Q. Zhou, Y.-L. Wang, B.-H. Liu, P. Shadbolt, Y.-S. Zhang, H. Gao, F.-L. Li, and J. L. O'Brien, "Quantum gambling based on nash-equilibrium," *npj Quantum Information*, vol. 3, no. 1, pp. 1–5, 2017.

[10] M. Houshmand, M. Houshmand, and H. R. Mashhadi, "Game theory based view to the quantum key distribution bb84 protocol," in *2010 Third International Symposium on Intelligent Information Technology and Security Informatics*. IEEE, 2010, pp. 332–336.

[11] S. C. Benjamin and P. M. Hayden, "Comment on "Quantum Games and Quantum Strategies"," *Physical Review Letters*, vol. 87, no. 6, p. 069801, 2001.

[12] "Prisoner's dilemma." [Online]. Available: https://en.wikipedia.org/wiki/Prisoner%27s_dilemma

[13] E. Mazumdar, L. J. Ratliff, and S. S. Sastry, "On gradient-based learning in continuous games," *SIAM Journal on Mathematics of Data Science*, vol. 2, no. 1, pp. 103–131, 2020.

[14] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, and H.-J. Briegel, "Entanglement in graph states and its applications," *arXiv preprint quant-ph/0602096*, 2006.

[15] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[16] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018.