Quantum Version of a Generalized Monty Hall Game and Its Possible Applications to Quantum Secure Communications

Luis Fernando Quezada and Shi-Hai Dong*

In this work, the authors propose a quantum version of a generalized Monty Hall game, that is, one in which the parameters of the game are left free and not fixed on its regular values. The developed quantum scheme is then used to study the expected payoff of the player, using both a separable and an entangled initial state. In the two cases, the classical mixed-strategy payoff is recovered under certain conditions. Lastly, the authors extend the quantum scheme to include multiple independent players, and use this extension to sketch two possible application of the game mechanics to quantum networks, specifically, two validated, multi-party, key-distribution quantum protocols.

1. Introduction

Due to its versatility, the area of mathematics known as game theory, which studies the strategies to be made by rational decision-makers in a conflict situation, has been proven useful to solve problems in a wide range of areas, including economics, biology, and computer science.[1–3] Motivated by these vast applications, and the recent development and commercial availability of quantum machines, quantum theorists start combining the game theory methodology with some features of quantum theory, such as superposition of states, projective measurements, and quantum entanglement,[4–14] leading to the creation of quantum game theory.

Applications of quantum game theory have already been found in the study of quantum coherence[15] and quantum mechanics foundations,[16] in a quantum-like description of markets and economics,[17] and in the development of quantum key-distribution protocols.[18] Furthermore, in 1999, Eisert et al. conjectured that “survival games” might be played by nature at a molecular level,[19] and in 2014, Bohl et al. concluded that classical game theory can correctly model some of the behaviors of viruses, genes, and proteins,[20] suggesting that smaller molecules can be considered as players in a quantum game. These results, along with the quantum mechanical description of protein folding,[21] could lead to potential applications of quantum game theory in medicine and biotechnology.

One of the games analyzed by quantum theorists was the one presented in the famous Monty Hall problem,[22–24] mainly because of its counter-intuitive result, which led to an intense discussion between numerous probability experts from 1975 to 1999. This game is particularly interesting from an information-theory perspective, since it illustrates how the application of a seemingly null operation over the system by one of the players provides information on it to the other player. In 2001, using a quantum version of the Monty Hall game, Li et al. found that quantum measurements could change the expected payoffs of the players, allowing a fair two-party zero-sum game to be carried out.[25] In 2016, Kurzyk and Glos constructed a quantum version of the Monty Hall problem based on a generalization of Bayesian networks, allowing them to show the difference between classical and quantum Bayesian reasoning.[26]

The development of a quantum game from its classical counterpart is completely subjective, although it is usually done by replacing the strategies and procedures of the classical game with elements present in the study of a quantum system, such as states, unitary operators and projective measurements. As a result of this, there are to date various approaches and different quantum versions of the Monty Hall game.[25–30]

In our previous work,[18] we proposed two quantum key-distribution protocols based on the quantum version of the regular Monty Hall game developed by Flitney and Abbott.[27] Since the regular Monty Hall game mechanics and parameters only allow the game to be played by two parties, the formalism in Flitney and Abbott's work could not be used to develop a multi-party quantum protocol. In this work, we focus on developing a quantum version of a generalized Monty Hall game, that is, one in which the parameters of the game are not fixed on its regular values, and analyze the players' expected payoffs under certain strategies. From this more general quantum scheme, we recover the classical results and analyze both a case in which the initial state of the game is separable, and one in which is entangled. Lastly, we extend our proposed scheme to include multiple independent players, and use this extension to sketch a possible application of the game mechanics to quantum networks.
The paper is organized as follows: A summary of the classical Monty Hall game results, as well as their generalization, are given in Section 2. In Section 3, we introduce the formalism of our proposed quantum scheme of the generalized game and present the results in Section 4. The separable case is studied in Section 4.1, while the entangled case is studied in Section 4.2. Lastly, in Section 5.1, we expose a multi-player version of our proposed quantum scheme, while in Sections 5.2 and 5.3, we sketch two possible applications of the multi-player game to quantum networks.

2. Classical Monty Hall Game

The Monty Hall problem, where the Monty Hall game is presented, is a puzzle in probability theory proposed in 1975[22,23] and actively discussed in 1991[24] due to its counter-intuitive result.

The mechanics of the game is as follows: In a contest, a player is asked to choose between three doors, behind one of which is a car (the prize) and the other two are goats. If the door chosen by the player is the one with the car behind, the host of the contest (Monty Hall), who knows where the car is, randomly opens one of the other two doors, revealing to the player one of the goats. If the door chosen by the player is the one with a goat behind, the host opens the only remaining door hiding a goat. The player is then asked if he wishes to open his initially chosen door or prefers to switch and open the other remaining closed door. It is found that the best strategy for the player to follow is to switch, as the probability of finding the car behind the door he initially chose is 1/3, while the probability of finding the car behind the other door is 2/3.

A simple but rigorous way to obtain the above result is the following: Both the location of the car and the initially chosen door by the player are random, independent events with a probability of 1/3 each. This means that the probability of simultaneously the car being behind door $j$ and the player initially choosing door $i$ is simply $P(i,j) = 1/9$ for all $i,j = 1, 2, 3$. Therefore, all the nine events of the corresponding sample space $\{(i,j)|i,j = 1, 2, 3\}$ have a probability of 1/9. Notice that the events of the form $(i,j)$ with $i = j$ are the cases in which the player wins if he decides to open his initially chosen door, while the events of the form $(i,j)$ with $i \neq j$ represent the cases in which the player wins if he decides to switch. The probability $P_{\text{ns}}$ of the player finding the prize by opening his initially chosen door is calculated by adding the probabilities of the elements corresponding to that event:

$$P_{\text{ns}} = P(1,1) + P(2,2) + P(3,3) = \frac{1}{3} \quad (1)$$

Analogously, the probability $P_s$ of the player finding the prize by switching doors is:

$$P_s = P(1,2) + P(1,3) + P(2,1) + P(2,3) + P(3,1) + P(3,2) = \frac{2}{3} \quad (2)$$

A possible generalization of the Monty Hall game can be made by considering an arbitrary number of doors $d$ to hide the prize and various not-prized doors to be opened by the host. In this case, the sample space corresponding to simultaneously the car being behind door $j$ and the player initially choosing door $i$ has the form $\{(i,j)|i,j = 1, \ldots, d\}$, and each element has a probability of $1/d^2$. Notice again that the $d$ events of the form $(i,j)$ with $i = j$ are the cases in which the player wins if he decides to open his initially chosen door; this means that the probability $P_{\text{ns}}$ of the player finding the prize by opening his initially chosen door is:

$$P_{\text{ns}} = \frac{1}{d} \quad (3)$$

On the other hand, the events of the form $(i,j)$ with $i \neq j$ have the same probability of $1/d^2$ to happen, but not of the player to win by switching. That can be calculated by considering that, after the host opens $m$ not-prized doors, there are $d - m - 1$ possible doors for the player to switch, meaning that each of the $(d - 1)$ events of the form $(i,j)$ with $i \neq j$ has a probability of $1/d^2(d - m - 1)$ of the player winning by switching. Thus, the probability of the player finding the prize by switching doors is:

$$P_s = \left(\frac{d - 1}{d - m - 1}\right) \frac{1}{d} \quad (4)$$

The game can be further generalized to be a multi-player one. Consider $n$ players (counting the host as a player) and suppose that all of them win the prize if they open the correct door, in this way, the players’ strategies are independent from each other’s, and expressions (3) and (4) remain the same for each one of them.

For consistency with the game mechanics, in this generalization scheme, the parameters $d$ (the total number of doors), $m$ (the not-prized doors to be opened by the host), and $n$ (the number of players including the host) are subject to the following restrictions:

$$n \geq 2 \quad (5)$$

$$d - n \geq m \geq 0 \quad (6)$$

It is worth mentioning that $P_s + P_{\text{ns}} = 1$ only when $d - n = m$.

3. Quantum Version of the Generalized Monty Hall Game

In this section, we propose a quantum version of the generalized Monty Hall game presented in Section 2. As it is usual in both quantum information and quantum game theory, we use the characters Alice and Bob as the host and the player respectively.

The states of the game will be described by normalized vectors $|\psi\rangle$ living in the space:

$$H = \bigotimes_{i=1}^{m+n} H_i \quad (7)$$

where $m$ is the number of not-prized doors to be opened by Alice (the host), $n$ is the number of players (counting the host as a
player), and every $H_i$ is the complex vector space of dimension $d$ (the total number of doors). Without loss of generality, and in order to simplify the game description, here we focus on the case $n = 2$ (i.e., the host and one player). Thus, we write a state of the game in the space $H$ as

$$|\psi\rangle = |\bar{o}, b, a\rangle = |o_m, \ldots, o_1, b, a\rangle$$

(8)

where $a \in \{0, \ldots, d-1\}$ indicates the door in which Alice hides the prize, $b \in \{0, \ldots, d-1\}$ the door chosen by Bob, and $o_i \in \{0, \ldots, d-1\}$ the not-prized doors to be opened by Alice.

The game mechanics creates some restrictions on the labels $a, b, o_i$. As we mentioned in Section 2, the location of the prize and the initial chosen door by the player are independent events; this means $a$ and $b$ can have any value in $\{0, \ldots, d-1\}$. However, in order for Alice to open $m$ different not-prized doors, the labels $o_i$ must be different from each other, that is, $o_i \neq o_j$ if $i \neq j$. Furthermore, the opened not-prized doors must also be different from the one where the prize is hidden and from the one selected by Bob, that is, $o_i \neq a, b$ for all $i$. We denote by $G$ the subspace of $H$ generated by all possible game states.

We consider the initial state of the game to be of the form

$$|\psi^{(0)}\rangle = |\bar{0}\rangle \otimes |\phi^{(0)}\rangle$$

(9)

where $|\phi^{(0)}\rangle$ is any state in the space corresponding to the prize’s location and Bob’s initially chosen door (labels $a$ and $b$), and $\bar{0}$ accounts for all the opened doors labels $o_i$ to be initially 0.

The game begins with Alice and Bob applying their strategies on the initial state $|\psi^{(0)}\rangle$. That is, Alice hides the prize behind a door by applying a special unitary operator $A$ on the first qudit (the one labeled as “a”), and Bob chooses a door by applying a special unitary operator $B$ on the second qudit (the one labeled as “b”). The next step is for Alice to open $m$ different not-prized doors, which is implemented by applying in succession the door-opening operators:

$$\hat{O}_j = \sum_{\bar{o}, b, a} \frac{\epsilon(a, b, \bar{o})}{\sqrt{d + 1 - j - U(a,b)}} \cdot |o_{j+1}, b, a\rangle \langle 0, o_{j+1}, b, a|$$

(10)

where the sum runs from 0 to $d - 1$, $j \in \{1, \ldots, m\}$, $\bar{o}_j$ stands for the ordered set of labels $(o_1, o_{k+1}, \ldots, o_m)$.

$$\epsilon(x) = \begin{cases} 0 & \text{if any two labels in } x \text{ have the same value}, \\ 1 & \text{otherwise} \end{cases}$$

(11)

and the $U$ function returns the number of unique elements in its argument. For example, $U(1, 3, 5) = 3$, while $U(0, 2, 2) = 2$.

Each of the possible $m$ door-opening operators $\hat{O}_j$ acts on the space corresponding to the labels $a, b, o_1, \ldots, o_m$ creating a superposition of all the possible doors to be opened, namely, the ones that remain after Alice and Bob have played their strategies and the ones that have not already been opened by the previous operators $\hat{O}_i$ with $k < j$. Furthermore, every $\hat{O}_j$ is a special unitary operator in its domain (states with $\bar{o}_j = 0$) and thus can be arbitrarily extended to be special unitary in all $H$.

Lastly, Bob decides whether he keeps his initial choice or prefers to switch it. The switching case can be implemented by applying the door-switching operator

$$\hat{S} = \frac{1}{\sqrt{d}} \sum_{\bar{o}, b} \epsilon(b, \bar{o}) \cdot |\bar{o}, b\rangle \langle b, \bar{o}|$$

(12)

where the sum runs again from 0 to $d - 1$, $b \oplus \epsilon_{k,\bar{o}}$ symbolizes the sum mod. $d$ and

$$\epsilon_{k,\bar{o}} = \min_{x \in \{1, \ldots, d-1\}} \{|k \mid (b \oplus k) \notin \bar{o}\}$$

(13)

The door-switching operator $\hat{S}$ acts on the space corresponding to the labels $b, o_1, \ldots, o_m$, changing label $b$ (Bob’s initially chosen door) to the next one (mod. $d$) available, that is, a door different from all the doors that have already been opened by the operators $\hat{O}_j$. Notice that $\hat{S}$ is also special unitary in its domain and hence it can be extended to be in all $H$.

We introduce a parameter $\gamma \in [0, \pi/2]$ to account for a quantum mixed strategy approach in the switching decision. This is implemented by Bob applying the operator

$$\cos \gamma \hat{I}_{d^{m+1}} + \sin \gamma \hat{S}$$

(14)

where $\hat{I}_{d^{m+1}}$ is the identity operator of dimension $d^{m+1}$. The factor $\sin \gamma$ represents the probability amplitude of Bob applying the door-switching operator $\hat{S}$, while $\cos \gamma$ represents the probability amplitude of Bob keeping his initial choice.

The final state of the game is therefore given by

$$|\psi^{(f)}\rangle = |(\cos \gamma \hat{I}_{d^{m+1}} + \sin \gamma \hat{S}) \otimes \hat{I}_b|$$

$$\times \prod_{j=0}^{m} (\hat{I}_{d^{m+1}} \otimes \hat{O}_j) \cdot (\hat{I}_{d^{m+1}} \otimes \hat{B} \otimes \hat{A}) |\psi^{(0)}\rangle$$

(15)

Bob wins if he opens the same door that Alice chose to hide the prize, that is, Bob wins if his qudit has the same value as Alice’s. Thus, the probability of Bob winning the game, that is, his expected payoff, is

$$\langle S_b \rangle = \sum_{j, \bar{o}} \left| \langle \bar{o}, i, i | \psi^{(f)}\rangle \right|^2$$

(16)

where, once again, the sum runs from 0 to $d - 1$.

Furthermore, as a non-cooperative game, Alice wins if Bob fails to choose the correct door. Therefore, her expected payoff is simply $\langle S_a \rangle = 1 - \langle S_b \rangle$.

It is worth mentioning that the quantum mixed strategy modelled by the parameter $\gamma$ in Equation (14) creates a superposition of the switching and not-switching cases, and thus is essentially different from a classical mixed strategy, where the expected payoff is given by $S = \cos^2 \gamma S_{\text{not-switch}} + \sin^2 \gamma S_{\text{switch}}$.

4. Results

4.1. Without Entanglement

In this section, we analyze the expected payoff of the player (Bob) when the initial state of the game (9) is not entangled. Specifically,
as usual in quantum game theory and quantum computation, we consider the initial state to be
\begin{equation}
|\psi^{(i)}\rangle = |\vec{0}\rangle \otimes |00\rangle
\end{equation}
where a, b, and all labels in \( \vec{0} \) are initialized at zero.

In this case, using Equations (15) and (16), and identifying the player’s strategies \( \hat{A} \) and \( \hat{B} \) with their respective matrix elements \( a_{i,j} \), \( b_{i,j} \), the expected payoff of Bob is found to be
\begin{equation}
\langle S_B \rangle = \frac{(d-m-1)!}{(d-1)!} \sum_{j,o} |a_{j,o}|^2 \cdot \cos \gamma \cdot b_{j,o} \cdot \epsilon (\vec{o}, j) \\
+ \sqrt{\frac{d-1}{d-m-1}} \sin \gamma \cdot b_{j,o} \cdot \epsilon (\vec{o}, j \oplus \lambda_{j,o}) \right|^2 
\end{equation}
where the sum runs from 0 to \( d-1 \), the symbol \( \oplus \) symbolizes the subtraction mod. \( d \), and the term \( \lambda_{j,o} \) is defined as
\begin{equation}
\lambda_{j,o} = \min_{k \in \{1, \ldots , d-1\}} \{ k | \ (j \oplus k) \notin \vec{o} \} 
\end{equation}

These strategies lead to the matrix elements in expression (18) to respectively be
\begin{equation}
a_{k,o} = \frac{1}{\sqrt{d}} 
\end{equation}
\begin{equation}
b_{k,o} = \delta_{ik}
\end{equation}
and represent the case in which Alice hides the prize in a homogeneous superposition of doors and Bob chooses a specific one.

**Figure 1** shows the classical-mixed-strategy’s behavior of Bob’s expected payoff \( \langle S_B \rangle \) as a function of the parameter \( \gamma \), obtained with a non-entangled initial state.

\begin{equation}
\langle S_B \rangle = \frac{P_m \cos^2 \gamma + P_s \sin^2 \gamma}{P_m + P_s}
\end{equation}

Notice that the mixed classical payoff in Figure 1 does not exceed the classical probability of winning by switching \( P_s \) for any value of \( \gamma \).

A particularly interesting case is where Bob’s strategy is to choose a homogeneous superposition of all possible doors, that is, choosing \( \hat{B} = \text{QFT} \), which leads to \( b_{k,o} = 1/\sqrt{d} \) for all \( k \). This results in Bob’s expected payoff in Equation (18) not depending on Alice’s strategy, and having the form
\begin{equation}
\langle S_B \rangle = \left| \sqrt{P_m} \cos \gamma + \sqrt{P_s} \sin \gamma \right|^2
\end{equation}

\begin{figure}
\centering
\includegraphics[width=0.5\textwidth]{figure1.png}
\caption{Classical-mixed-strategy’s behavior of Bob’s expected payoff \( \langle S_B \rangle \) as a function of the parameter \( \gamma \), obtained with a non-entangled initial state.}
\end{figure}

\begin{figure}
\centering
\includegraphics[width=0.5\textwidth]{figure2.png}
\caption{Bob’s expected payoff \( \langle S_B \rangle \) as a function of the parameter \( \gamma \), obtained with a non-entangled initial state and using \( \hat{B} = \text{QFT} \). The curve is independent of Alice’s strategy.

Figure 2 shows the plot of expression (24) as a function of the parameter \( \gamma \). It can be seen that, in this case, \( \langle S_B \rangle \) has a maximum value of
\begin{equation}
\langle S_{B,max} \rangle = \left| \frac{P_m}{\sqrt{P_m + P_s}} + \frac{P_s}{\sqrt{P_m + P_s}} \right|^2
\end{equation}
at
\begin{equation}
\gamma_{\text{max}} = \arctan \left( \sqrt{\frac{P_m}{P_s}} \right)
\end{equation}
which is greater than \( P_s \) (the maximum value attainable by a classical strategy), meaning that, in this particular game, access to quantum strategies leads to a greater payoff. Furthermore, if \( P_m + P_s = 1 \), then \( \langle S_{B,max} \rangle = 1 \). This means that, by choosing the strategies \( \hat{B} = \text{QFT} \) and \( \gamma = \gamma_{\text{max}} \), Bob can win every time regardless of Alice’s strategy. Therefore, in this latter case, the set of strategies \( \{ \hat{A} \in \text{SU}(d) | \hat{B} = \text{QFT}, \gamma = \gamma_{\text{max}} \} \) conforms a quantum weak Nash equilibrium.

The graphics in Figures 1 and 2 can be seen as the extreme cases of the family of curves obtained by varying Bob’s
strategy when Alice’s strategy is fixed at $\hat{A} = \text{QFT}$. Figure 3 shows, for the case $d = 5$, $m = 1$, a subset of this family of curves when $\hat{A} = \text{QFT}$, and (bottom up) $B |0\rangle = |0\rangle$, $\hat{B} |0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$, $\hat{B} |0\rangle = \frac{1}{\sqrt{1}} (|0\rangle + |1\rangle + |2\rangle)$. $\hat{B} |0\rangle = \frac{1}{\sqrt{4}} (|0\rangle + |1\rangle + |2\rangle)$ and $\hat{B} = \text{QFT}$. We can see from expression (18) that the more doors are included in the superposition of Bob’s strategy (more $b_{0,j} \neq 0$), the closer the curve is going to be to the case where $\langle S_B \rangle_{\text{max}}$ is reached.

4.2. With Entanglement between Host and Player

In this section, we analyze the expected payoff of the player (Bob) when the initial state between him and the host (Alice), $|\psi\rangle$ in Equation (9) is entangled. Specifically, we consider the state $|\psi\rangle$ to be the GHZ state [31] of dimension $d$ between two parties:

$$|\psi^{(0)}\rangle = \sum_{j=0}^{d-1} |j\rangle$$

leading the initial state of the game (9) to be

$$|\psi^{(0)}\rangle = |\bar{0}\rangle \otimes \sum_{j=0}^{d-1} |j\rangle$$

In this case, using Equations (15) and (16), and identifying the player’s strategies $\hat{A}$, $\hat{B}$ with their respective matrix elements $a_{i,j}$, $b_{j,k}$, the expected payoff of Bob is found to be

$$\langle S_B \rangle = \frac{(d - m - 1)!}{d!} \cdot \sum_{j=0}^{d-1} \cos \gamma \cdot \epsilon(\bar{0}, j) \cdot \sum_{i=1}^{d} (a_{ij} \cdot b_{jk})$$

$$+ \sqrt{\frac{d - 1}{d - m - 1}} \sin \gamma \cdot \epsilon(\bar{0}, j \otimes \lambda_{j,k}) \sum_{i=1}^{d} (b_{j,i} \cdot a_{ij})^2$$

where the sums run from 0 to $d - 1$.

A first interesting result is obtained when both Alice and Bob apply the quantum Fourier transform, namely,

$$a_{j,k} = b_{j,k} = \frac{1}{\sqrt{d}} e^{\frac{2\pi i j k}{d}}$$

In contrast with the obtained expected payoff in the non-entangled case (24), the extra phase in the matrix elements leads to the terms that combine the cosine and the sine in expression (29) to cancel, resulting in the entangled expected payoff to be the same as the classical one, that is, the one in Equation (23).

The GHZ state perfectly correlates Alice and Bob’s labels, meaning that if neither Alice nor Bob applies a strategy ($\hat{A} = \hat{B} = \hat{I}_d$), Bob will win with a probability of 1 if he decides not to apply the door-switching operator, and with a probability of 0 if he decides to apply it. The above can be regarded as a particular case of both labels being displaced by a fixed amount $k \in \{0, \ldots, d - 1\}$, which can be implemented by Alice and Bob respectively applying the strategies introduced in Equation (20), specifically $\hat{A} = \text{SUM}_d(i)$ and $\hat{B} = \text{SUM}_d(i + k)$ for any $i$. In this case, the expected payoff is found to be

$$\langle S_B \rangle = P_{n,k} \cos^2 \gamma + P_{k} \sin^2 \gamma$$

where

$$P_{n,k} = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases}$$

$$P_{k} = \begin{cases} m! (k - 1)! & \text{if } k \geq d - m - 1 \\ (m + k + 1 - d)! (d - 2)! & \text{if } k < d - m - 1 \end{cases}$$

Figure 4 shows, for the case $d = 6$ and $m = 3$, Bob’s expected payoff obtained using a displacement of $k = 0, 1, 2, 3, 4, 5$. Notice that $\langle S_B \rangle$ in Equation (31) strongly depends on the specific displacement $k$, as well as in the difference between the total number of doors $d$ and the number of doors to be opened $m$. This is due to how the door-opening operators $\hat{O}_j$ and the door-switching...
operator \( \hat{S} \) work. The door-opening operators will begin to “fill the gaps” between Alice and Bob’s displaced labels, allowing the door-switching operator to “jump” from Bob’s initial label to Alice’s one, resulting in a greater probability of winning by switching when the displacement is closest (from below) to \( d \), being the extreme cases \( k = 0 \) (perfect correlation) and \( k = d - 1 \), where there are no gaps to fill and the door-switching operator automatically switches Bob’s label to Alice’s one. However, if the number of doors to be opened \( m \) is not large enough to fill the gaps created by the displacement \( k \), that is, \( m < d - k - 1 \), the door-switching operator will not be able to jump from Bob’s label to Alice’s, resulting in Bob’s expected payoff to be zero regardless of the value of \( \gamma \).

In general, as Flitney and Abbott mentioned in their quantum scheme of the regular game,\(^{27}\) if the initial state is the one in Equation (28), then the game does not have a Nash equilibrium where

\[
\begin{align*}
\text{Ann. Phys. (Berlin) 2021, 533, 2000427} & \text{ www.advancedsciencenews.com www.ann-phys.org} \\
\text{© 2020 Wiley-VCH GmbH}
\end{align*}
\]

Furthermore, since every player is independent from each other, they all need a door-switching operator of their own, namely,

\[
\hat{S}_k = \sum_{\hat{o}, \hat{p}_k} \epsilon (\hat{o}, \hat{p}_k) \cdot |\hat{o}_k, \hat{p}_k \rangle \langle \hat{o}_k, \hat{p}_k| \tag{37}
\]

with \( k \in \{2, \ldots, n\} \). Each operator \( \hat{S}_k \) acts on the space corresponding to the labels \( o_1, \ldots, o_m, p_k \), that is, it only switches the door initially chosen by player \( P_k \) and does not consider the doors chosen by other players at all. Hence, the results from the previous sections apply the same to each player.

5.2. Direct Application

Using the new definitions of the previous subsection, we are now in a position to sketch a direct application of the game, using the same operators and mechanics. We first propose a validated multi-party quantum key-distribution protocol in a trusted network, in which the host (\( P_1 \)) acts as a central node and distributes the key to the \( n - 1 \) players \( P_2, \ldots, P_n \), while other \( m \) parties, which we will denote as \( V_1, \ldots, V_m \), validate the distribution. It is worth mentioning that the protocol proposed in this subsection is not intended to be a secure way of distributing a random key, but rather a secure way of validating the distribution.

The protocol is developed under the condition \( d = m + 2 \) and goes as follows:

1) \( P_1 \) generates the state

\[ |\psi\rangle = |\bar{0}, \bar{0}\rangle \tag{38} \]

that is, the state where all the \( m \) labels in \( \bar{o} \) and all the \( n \) labels in \( \bar{p} \) are equal to zero.

2) \( P_1 \) sends the qudits \( p_1, \ldots, p_n \) to the respective \( n - 1 \) players \( P_2, \ldots, P_n \), and keeps the qudits \( p, p_k \) and all the ones in \( \bar{o} \).

3) Each participant \( P_k \) \( (k = 1, \ldots, n) \) randomly applies, to its own qudit, one of the following two strategies: \( \hat{P}_k = \text{SUM}_m(0) \), \( \hat{P}_k = \text{SUM}_d(1) \), and privately stores in a classical bit \( b_k \), its selection: \( b_k = 0 \) for \( \text{SUM}_m(0) \) and \( b_k = 1 \) for \( \text{SUM}_d(1) \).

4) All the players send back the qudits \( p_1, \ldots, p_n \) to \( P_1 \).

5) \( P_1 \) sends all the state to the first validation party \( V_1 \).

6) \( V_1 \), based on some authentication or relevant information related to the transaction, applies (or not) its own door-opening operator, and sends the state to the next validation party \( V_2 \). This procedure continues until all validation parties \( V_1, \ldots, V_m \) have decided to validate (apply the corresponding door-opening operator) or not the key distribution.

7) \( V_m \) sends back the full state to \( P_1 \).

8) Each player randomly chooses to switch (s) or not (ns) his initial choice. This information is then made public for \( P_1 \) to have it.

9) Based on the information from the previous step, \( P_1 \) applies or not the corresponding door-switching operators \( \hat{S}_k \).

10) \( P_1 \) measures the \( n \) qudits corresponding to the labels in \( \bar{p} \), and publicly announces which players won (w) and which ones lost (l).
It is worth mentioning that there exist specific cases in which the protocol will not work, namely, when \( p_1 = p_2 = \cdots = p_n \). This is satisfied when all \( \mathcal{P}_1, \ldots, \mathcal{P}_n \) applied the same strategy, that is, either \( b_1 = \cdots = b_n = 0 \) or \( b_1 = \cdots = b_n = 1 \). However, the probability of the host and all players applying the same strategy is \( 1/2^{n-1} \), which decreases exponentially with the number of players \( n \) and, thus, can be considered an unlikely error for large networks.

It should be mentioned that in order for all the players \( \mathcal{P}_1, \ldots, \mathcal{P}_n \) to share the same key at the end of the protocol, it is necessary that all validation parties \( \mathcal{V}_1, \ldots, \mathcal{V}_n \) apply their corresponding door-opening operator, that is, the validation parties function is to approve the key distribution. The criteria for approval would of course depend on the specific scenario where the protocol is used; it may be some background information regarding the players or simply the will of a person.

### 5.3. Motivated Application

Motivated by some of the key features of the quantum version of the generalized multi-player Monty Hall game, in this subsection, we propose another validated multi-party quantum key-distribution protocol. Unlike the one proposed in the previous subsection, where the validation procedure is the one protected by the remaining state’s entanglement, in this protocol validation itself plays a secondary role, and the distribution of the key is the one protected by entanglement.

The protocol is developed under the conditions \( d = m + 2 = n + 1 \) and goes as follows:

1) \( \mathcal{P}_1 \) generates the state

\[
|\psi\rangle = |\tilde{0}\rangle \otimes \sum_{i=0}^{d-1} |i\cdots i\rangle
\]  

(40)

that is, the state where all the labels in \( \tilde{a} \) are equal to zero, and the players’ qudits \( \tilde{p} \) are prepared in the GHZ state of dimension \( d \) between \( n \) parties.

2) \( \mathcal{P}_1 \) sends the qudits \( p_1, \ldots, p_n \) to the respective \( n-1 \) players \( \mathcal{P}_2, \ldots, \mathcal{P}_n \), and keeps the qudits \( p_1 \) and all the ones in \( \tilde{a} \).

3) Each participant \( \mathcal{P}_k \) \((k = 1, \ldots, n) \) randomly applies, to its own qudit, one of the following two strategies: \( \tilde{P}_k = \text{SUM}_d(0) \), \( \tilde{P}_k = \text{SUM}_d(1) \), and privately stores in a classical bit \( b_1 \) its selection: \( b_1 = 0 \) for \( \text{SUM}_d(0) \) and \( b_1 = 1 \) for \( \text{SUM}_d(1) \).

4) All the players send back the qudits \( p_2, \ldots, p_n \) to \( \mathcal{P}_1 \).

5) \( \mathcal{P}_1 \) sends qudits \( p_1 \) and \( a_{\tilde{j}-1} \) to the corresponding validation party \( \mathcal{V}_{\tilde{j}-1} \) for all \( j \in \{2, \ldots, n\} \).

One of the key features of the door-opening operators defined in Equation (10) is the gap-filling property discussed in Section 4.2. Here, we define a simpler variation of the door-opening operators that preserves the gap-filling property without creating the superposition of all possible combinations of opened doors, namely,

\[
\hat{O}_j = \sum_{i=0}^{d-1} |i \oplus j, i\rangle\langle 0, i|
\]  

(41)
where \( j \in \{2, \ldots , n\} \). Operators \( \hat{\Omega}_j \) act on the space corresponding to the labels \( o_{j-1} \) and \( p_j \), and are special unitary in their domain (states with \( o_{j-1} = 0 \)).

6) For all \( j \in \{2, \ldots , n\} \), validation party \( \mathcal{V}_j \), based on some authentication or relevant information related to the transaction, applies (or not) its own variation of the door-opening operator \( \hat{\Omega}_{j-1} \), and sends back qudits \( o_{j-1} \) and \( p_j \) to \( P_j \).

7) Each player randomly chooses to switch (s) or not (ns) his initial choice. This information is then made public for \( P_j \) to have it.

8) Based on the information from the previous step, \( P_j \) applies or not the corresponding door-switching operators \( S_j \).

In order to know which players won (w) and which ones lost (l), without measuring their qudits (which would make the initial entanglement of the GHZ state disappear), we use the same strategy as in ref. [18] That is, we define victory-encoding operators \( \hat{V}_j \), whose function is to encode in qudit \( o_{j-1} \) the result of player \( P_j \):

\[
\hat{V}_j = \sum_{i,k} (\delta_{i,k;01} + \delta_{i,k} + \delta_{i,k;01}) \cdot |i-j,i,k\rangle\langle i,j,i,k|
\]

where the sum runs form 0 to \( d - 1 \), \( \delta_{i,k} \) stands for Kronecker’s delta and \( j \in \{2, \ldots , n\} \). Operators \( \hat{V}_j \) act on the space corresponding to the labels \( o_{j-1} \), \( p_j \) and \( p_1 \), and are special unitary in their domain (states with \( p_1 = p_1 \oplus 1 \), \( p_j = p_j \) or \( p_j = p_1 \oplus 1 \)).

Notice that, after the application of the victory-encoding operator \( \hat{V}_j \), the case where player \( P_j \) won (\( p_1 = p_j \)) results in \( o_{j-1} = 0 \), while the case in which \( P_j \) lost \( p_j \neq p_1 \) results in \( o_{j-1} = 1 \).

9) \( P_j \) applies the \( n - 1 \) victory encoding operators \( \hat{V}_j \) to the corresponding qudits.

10) \( P_j \) measures the \( m \) qudits corresponding to the labels in \( \bar{\sigma} \), and publicly announces which players won (w) and which ones lost (l).

11) Knowing the game results, the players who had switched (s) and won (w), or not switched (ns) and lost (l), negate their bit \( b_k \) from step 3.

Figure 6 shows a scheme of the protocol proposed in this subsection. The protocol works due to the gap-filling property of the operators \( \hat{\Omega}_j \), while its security relies on the encoding function of the victory-encoding operators \( \hat{V}_j \). As in the protocol of the previous subsection, for each player \( P_j \) there are exactly eight possible results:

\[(b_1 = 1, b_k = 1, s, l),\]
\[(b_1 = 1, b_k = 1, ns, w),\]
\[(b_1 = 0, b_k = 1, s, w),\]
\[(b_1 = 0, b_k = 1, ns, l),\]
\[(b_1 = 1, b_k = 0, s, w),\]
\[(b_1 = 1, b_k = 0, ns, l),\]

Figure 6. Scheme describing a validated, multi-party, key-distribution, quantum protocol. The key-distribution procedure is protected from eavesdropping via the entanglement of the remaining state.

\[(b_1 = 1, b_k = 1, s, l).\]

(43)

Notice again that the cases switched (s) and won (w), and not switched (ns) and lost (l), are precisely the ones in which the host \( P_1 \) and the player \( P_j \) did not apply the same strategy (i.e., \( b_1 \neq b_k \)), and hence the need of step 11. At the end of the protocol, if all the validation parties applied their corresponding variation of the door-opening operator, the host and all players will share the same value on their bit \( b_1 \), and the game can be repeated depending on the desired length of the key. Furthermore, after the measurements performed in step 10, the remaining state, corresponding to the players’ labels in \( \bar{\sigma} \), is maximally entangled in a state equivalent to the GHZ state, and thus it can be used in a Bell-type test to ensure the key distribution was done without external intervention.

It should be mentioned that, as in the protocol of the previous subsection, in order for all the players \( P_1, \ldots , P_n \) to share the same key at the end of the protocol, it is necessary that all validation parties \( \mathcal{V}_1, \ldots , \mathcal{V}_n \) apply their corresponding variation of the door-opening operator. However, unlike the previous protocol, here the relevant feature is the key distribution, and thus the validation procedure (steps 5 and 6) can be completely omitted, simply by allowing the host to apply the operators \( \hat{\Omega}_j \). It is also worth mentioning that the protocol propose in this subsection will not work when \( p_1 = p_2 = \cdots = p_n \), but since the probability of this to happen is \( 1/2^{n-1} \), which decreases exponentially with the number of players \( n \), it may be considered as an unlikely error for large networks.

6. Discussion and Conclusions

In this work, we developed a quantum version of a generalization of the Monty Hall game. In the case where a non-entangled initial state is used, we recover the classical expected payoff by allowing the host to hide the prize in a homogeneous superposition of doors, and the player to choose only one of them. We also showed that, by using a superposition of the switching and not-switching decision, it is possible to exceed the classical probabilities for the

\[
\text{Ann. Phys. (Berlin) 2021, 533, 2000427}
\]
\[
\text{2000427 (8 of 9)}
\]
player to win. Furthermore, a quantum weak Nash equilibrium is found in a set independent of the host’s strategy.

When an entangled GHZ state is used as the initial state of the game, the classical result can be again recovered via a destructive interference caused by the host and the player both using the quantum Fourier transform as their strategy. We also showed that a displacement of the correlation present in the GHZ state, depending on the parameters values, can lead to a very marked difference between the switching and not-switching cases.

In both the separable and entangled initial-state cases, the importance of the number of doors to be opened by the host plays a significant role in the player’s expected payoff. In the separable case, it is decisive in the maximum value the payoff can have, while in the entangled case, the fewer doors are opened, the greater the cases in which the player cannot win regardless of his strategy. The heavy dependence of the player’s payoff with this parameter was the reason we decided not to treat it as a host’s possible strategy, nonetheless this is a case we would like to address in a future work.

In the last section, we extend our quantum scheme of the game to include multiple independent players, and use this extension to sketch two validated, multi-party, key-distribution, quantum protocols. The first protocol is proposed as a direct application of the multi-player quantum Monty Hall game, in the sense that it uses the same operators and mechanics. On the other hand, the second proposed protocol is less faithful to the game, as it only uses some of its key features to accomplish its purpose. Both protocols are protected by the entanglement of a remaining state, which can be used in a Bell-type test to ensure there was no external intervention in some specific steps: the validation procedure in the case of the first protocol, and the key distribution in the case of the second protocol.

We conclude that the mechanics of quantum games, or the quantum versions of some classical games, apart from being interesting from a basic-science perspective, can provide some useful insight in the search for a solution to multiple kinds of problems in applied quantum mechanics, particularly in the area of quantum information.

Acknowledgements

The authors would like to thank the referees for making invaluable and positive suggestions and criticisms, which have improved the manuscript greatly. This work was supported by SEP-CONACyT under project no. 288856 and partially by 20200981-SIP-IPN, Mexico. S.-H.D. is currently on sabbatical leave from IPN.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

entangled states, Monty Hall game, quantum networks

Received: August 28, 2020
Revised: October 14, 2020
Published online: November 10, 2020

[1] The Prize in Economic Sciences 2014. NobelPrize.org. Nobel Media AB 2020, https://www.nobelprize.org/prizes/economic-sciences/2014/summary/ (accessed September 2020).
[2] J. M. Smith, in Evolution and the Theory of Games, Cambridge University Press, Cambridge 1982.
[3] S. N. Durlauf, L. E. Blume, in Computer Science and Game Theory (Eds: S. N. Durlauf, L. E. Blume), The New Palgrave Economics Collection, Palgrave Macmillan, London 2010.
[4] D. A. Meyer, Phys. Rev. Lett. 1999, 82, 1052.
[5] S. C. Benjamin, P. M. Hayden, Phys. Rev. Lett. 2001, 87, 069801.
[6] J. Eisert, M. Wilkens, M. Lewenstein, Phys. Rev. Lett. 2001, 87, 069802.
[7] S. C. Benjamin, P. M. Hayden, Phys. Rev. A 2001, 64, 030301(R).
[8] S. J. van Enk, R. Pike, Phys. Rev. A 2002, 66, 024306.
[9] A. P. Fitzney, D. Abbott, Fluct. Noise. Lett. 2002, 02, R175.
[10] A. P. Fitzney, D. Abbott, Proc. R. Soc. A 2003, 459, 2463.
[11] A. P. Fitzney, D. Abbott, J. Phys. A: Math. Theor. 2005, 38, 449.
[12] A. P. Fitzney, L. C. L. Hollenberg, Phys. Lett. A 2007, 363, 381.
[13] C. D. Hill, A. P. Fitzney, N. C. Menicucci, Phys. Lett. A 2010, 374, 3619.
[14] J. M. Chappell, A. Igbal, D. Abbott, Phys. Lett. A 2010, 374, 4104.
[15] C. F. Lee, N. F. Johnson, F. Rodriguez, L. Quiroga, Fluct. Noise. Lett. 2002, 02, L293.
[16] D. Rajan, M. Visser, Quant. Rep. 2020, 2, 39.
[17] E. W. Piotrowski, J. Sladkowski, Phys. A 2002, 312, 208.
[18] L. F. Quezada, S. H. Dong, Ann. Phys. 2020, 532, 2000126.
[19] J. Eisert, M. Wilkens, M. Lewenstein, Phys. Rev. Lett. 1999, 83, 3077.
[20] K. Bohl, S. Hummert, S. Werner, D. Basanta, A. Deutsch, S. Schuster, G. Theißeng, A. Schroetera, Mol. Biosyst. 2014, 10, 3066.
[21] L. Luo, Sci. China Phys. Mech. Astron. 2014, 57, 458.
[22] S. Selvin, M. Bloxham, A. I. Khuri, M. Moore, R. Coleman, G. R. Bryce, J. A. Hagans, T. C. Chalmers, E. A. Maxwell, G. N. Smith, Am. Stat. 1975, 29, 67.
[23] J. Dickey, N. T. Gridgeman, M. C. S. Kingsley, I. J. Good, J. E. Carlson, D. Gianola, M. H. Kutner, S. Selvin, Am. Stat. 1975, 29, 131.
[24] M. van Savant, J. P. Morgan, N. R. Chaganty, R. C. Dahiga, M. J. Doviak, N. R. Farnum, D. K. H. Fong, Am. Stat. 1991, 45, 347.
[25] C. F. Li, Y. S. Zhang, Y. F. Huang, G. C. Guo, Phys. Lett. A 2001, 280, 257.
[26] D. Kurzyk, A. Glos, Quantum Inf. Process. 2016, 15, 4927.
[27] A. P. Fitzney, D. Abbott, Phys. Rev. A 2002, 65, 062318.
[28] G. M. D’Ariano, R. D. Gill, M. Keyl, B. Kuemerer, H. Maassen, R. F. Werner, Quant. Inf. Comput. 2002, 2, 355.
[29] S. Khan, M. Ramzan, M. K. Khan, Commun. Theor. Phys. 2010, 54, 47.
[30] L. F. Quezada, A. Martin-Ruiz, A. Frank, E. Nahmad-Achar, Phys. Scr. 2020, 95, 065102.
[31] D. M. Greenberger, in Compendium of Quantum Physics (Eds: D. Greenberger, K. Hentschel, F. Weinert), Springer, Berlin–Heidelberg 2009.