Quantum Information Processing (2019) 18:171
https://doi.org/10.1007/s11128-019-2279-5

Dimensionality distinguishers

Nayana Das[1] · Goutam Paul[2] · Arpita Maitra[3]

Received: 29 October 2018 / Accepted: 9 April 2019 / Published online: 22 April 2019

Abstract
The celebrated Clauser, Horne, Shimony and Holt (CHSH) game model helps to perform the security analysis of many two-player quantum protocols. This game specifies two Boolean functions whose outputs have to be computed to determine success or failure. It also specifies the measurement bases used by each player. In this paper, we generalize the CHSH game by considering all possible non-constant Boolean functions and all possible measurement basis (up to certain precision). Based on the success probability computation, we construct several equivalence classes and show how they can be used to generate three classes of dimension distinguishers. In particular, we demonstrate how to distinguish between dimensions 2 and 3 for a special form of maximally entangled state.

Keywords CHSH · Dimensionality testing · Distinguisher · Entanglement · Success probability

1 Introduction

In quantum entanglement, two or more quantum particles (may be space-like separated) share their states in such a way that the state of each of the particles cannot be fully described without considering the other(s). If we change the quantum state of one particle thorough local unitary operations, the state of the rest of the par-

✉ Goutam Paul
goutam.paul@isical.ac.in

Nayana Das
dasnayana92@gmail.com

Arpita Maitra
arpita76b@gmail.com

1 Applied Statistics Unit, Indian Statistical Institute, Kolkata 700108, India

2 Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata 700108, India

3 Indian Institute of Technology Kharagpur, Kharagpur 721302, India

ticles changes automatically to maintain the entanglement. Many modern quantum protocols are based on entanglement theory, for example, quantum cryptography with Bell theorem [1], super-dense coding [2], quantum teleportation [3], entanglement swapping [4], etc. Most of them use maximally entangled states. The Bell states are special cases of bipartite maximally entangled states on Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ given by $|\psi\rangle = U_A \otimes U_B |\phi_d^+\rangle_{AB}$, where $|\phi_d^+\rangle = \sum_{i=1}^{d} \frac{1}{\sqrt{d}} |i\rangle \otimes |i\rangle$ [5].

In 1935, Einstein, Podolsky and Rosen (EPR) showed that quantum mechanics is not complete [6]. They also claimed that there may exist some local hidden variable theory, without requiring immediate action at a distance. Bell (1964) proposed a test for the existence of these hidden variables and developed an inequality [7], and he showed that if the inequality is not satisfied, then a local hidden variable theory would not be possible. Inspired by Bells paper, Clauser, Horne, Shimony and Holt (CHSH) (1969) formed a correlation inequality and Bell's theorem can be proved by using that inequality [8]. The CHSH inequality gives a bound on any local hidden variable model (LHVM). Cirel'son [9] showed that Bell inequalities can be violated by quantum mechanical correlations. Aspect et al. [10] showed some experimental results, on the CHSH inequality, which agree with the quantum mechanical predictions. Popescu and Rohrlich [11] formed some correlations, using no-signaling condition, violate the CHSH inequality even more than quantum mechanical correlations. A simple setting for showing the usefulness of entanglement involves a two-player game known as the CHSH game [12,13]. Buhrman [14] generalized the CHSH game in the field F_q. Some modern variants of CHSH appears in [15–19].

1.1 Why dimensionality testing is important?

For a physical system, we generally assume that it has a particular dimension. Any practical application that uses entangled quantum systems have some predefined dimensional entangled states. In information theory, the dimensionality of quantum systems is a resource. In cryptographic applications, the security level scheme depends on the dimension. So testing dimensionality or distinguishing dimensionality of the underlying state-space are important pre-processing tasks before executing the actual protocol.

Higher dimension implies more degrees of freedom. For example, consider Quantum Key Distribution (QKD) protocol with qubit. In this case, the legitimate parties use only polarization of a photon for encoding. However, they have to fix the values for the other degrees of freedom such as spectral line, spatial mode or temporal mode, etc. Lack of knowledge of any of these parameters may cause security back-door. Recently, Maitra et al. [35] showed that if the honest party measures only the polarization of a photon and remains ignorant about the *Orbital Angular Momentum* (OAM), then by changing the value of OAM one can steal more information than what he/she is entitled to in a certain type of QKD protocol. This strengthens the motivation of dimensionality testing.

1.2 How to test the dimensionality?

The dimension witness gives a bound on the dimension of an unknown system based on measurement statistics. It was first introduced for quantum systems in the context of non-local correlations by Brunner et al. [20] and further developed in [21–29]. Various experiments have been recently proposed about the implementation of such witnesses [30,31].

Some theory of dimensional detection of an unknown quantum system is based on the set of conditional probabilities. It is based on the analysis on the probabilities of observing an outcome after creating and measuring the system for a given set of possibilities. It has become a prominent research area in recent times [27–29]. Experimental tests for testing dimension of a quantum system have been explored [31,32], and it has produced successful results.

A simple and general dimension witnesses for quantum systems of arbitrary Hilbert space dimension was proposed by Brunner (2013) [33]. Their proposed work can distinguish between classical and quantum systems of the same dimension. A simple method for generating nonlinear dimension witnesses for systems of arbitrary dimension has been proposed by Bowles (2014) [34]. It has been shown in this paper that this witness can be used to certify the presence of randomness.

1.3 Our contributions

In this paper, we generalize the CHSH game and define two classes of new games which are similar to the CHSH game. The first one is for 2-variables and the second one is for 3-variables. In this class of new games, we change the winning condition of the CHSH game. Instead of a particular Boolean function in the CHSH game, we use all non-constant Boolean functions and find equivalence class for function pairs and bases such that all the elements of the same class have the same winning probability of the game. We also consider all possible measurement subjects to a precision parameter. For both the games, we optimize the winning probabilities. Finally, we show how our results can be used to devise three classes of dimensionality distinguishers, particularly between dimensions 2 and 3.

The efficiency of a distinguisher depends on the number of samples (for a given success probability) and that in turn depends on the gap between the probabilities. This issue has been discussed in detail in [36]. Moreover, there are some works [37] on how to deal with finite number of samples. In the current work, we do not focus on these types of analysis. Rather, our main goal is to identify the distinguishing events with a significant probability gap and that is what we report here.

2 Entanglement and the CHSH game

A special type of entangled states are maximally entangled states. There are many quantum protocols which use these maximally entangled states. One of them is the CHSH game, and we discuss about it.

2.1 Maximally entangled state

Let us take a Hilbert space H (for now, $H = \mathbb{C}^2$). There are infinitely many maximally entangled states in $H \times H$, and all are connected by a unitary. A pure bipartite state in $\mathbb{C}^2 \times \mathbb{C}^2$ is maximally entangled if the reduced density matrix is $\frac{I}{2}$ for both sub systems.

Let $|\phi\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle$ and $|\theta\rangle = \cos\beta\,|0\rangle + \sin\beta\,|1\rangle$. Then $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}[|\phi\theta\rangle + |\phi^{\perp}\theta^{\perp}\rangle] = \frac{1}{\sqrt{2}}[|0\rangle\,|\varphi\rangle + |1\rangle\,|\varphi^{\perp}\rangle]$, where $|\varphi\rangle = \cos(\alpha-\beta)\,|0\rangle - \sin(\alpha-\beta)\,|1\rangle$ is maximally entangled as $\rho_A = \rho_B = \frac{I}{2}$ where ρ_A and ρ_B are reduced density matrix of subsystem A and B, respectively.

Again let $|\chi\rangle_{AB} = \frac{1}{\sqrt{2}}[|0\rangle\,|\sigma\rangle + |1\rangle\,|\varrho\rangle]$ where $|\sigma\rangle = \cos\gamma\,|0\rangle + \sin\gamma\,|1\rangle$ and $|\varrho\rangle = \cos\delta\,|0\rangle + \sin\delta\,|1\rangle$. To make $\rho_A = \rho_B = \frac{I}{2}$, we must have $|\varrho\rangle = |\sigma^{\perp}\rangle$.

Thus a general form of maximally entangled state in $\mathbb{C}^2$ is $\frac{1}{\sqrt{2}}[|\phi\theta\rangle + |\phi^{\perp}\theta^{\perp}\rangle]$ (we are considering real coefficients only).

A maximally entangled (pure) state in a d-dimensional Hilbert space has the Schmidt decomposition $\sum_{i=1}^{d}\frac{1}{\sqrt{d}}\,|i\rangle \otimes |i\rangle$ in an appropriate basis. In Hilbert space $\mathbb{C}^m \otimes \mathbb{C}^n$ (say, $m < n$), a maximally entangled (pure) state is the same as that in $\mathbb{C}^m \otimes \mathbb{C}^m$.

2.2 The CHSH game

In this game, there are two players, namely Alice and Bob, and a referee. Let us assume that Alice and Bob are far away from each other and not able to communicate during the game. Before the game begins, they can communicate freely to discuss their strategy. During the game, they only communicate with the referee in the following way:

- The referee chooses two independent random bits x and y uniformly (also called questions) and sends x to Alice and y to Bob, i.e., for all $s \in \{0,1\}$, $t \in \{0,1\}$, $\Pr(x = s, y = t) = \Pr_{xy}(s,t) = \frac{1}{4}$.
- Alice and Bob reply to referee with bits a and b, respectively.
- Referee calculates $x \wedge y$ and $a \oplus b$ (where $\wedge$, $\oplus$ stand for AND and XOR operations, respectively)
- Alice and Bob win if $x \wedge y = a \oplus b$.

Their goal is to achieve the highest winning probability together. Classically, the winning probability is 0.75. But in the quantum world, this probability is 0.85 if they follow the strategy discussed in the following Sect. 2.2.1.

2.2.1 Quantum strategy

The strategy to win the game with maximum probability is to share a maximally entangled state (e.g., Bell state) between Alice and Bob. According to the referee's

questions, they choose measurement bases to measure their qubits and send their answers to the referee. Details are given in Algorithm 1. The values of θ_0 and θ_1 (defined in Algorithm 1) are fixed for CHSH game and those values are $\theta_0 = \frac{\pi}{8}$, $\theta_1 = \frac{15\pi}{8}$.

2.2.2 Winning probability

Let win be the event that Alice and Bob win, i.e., $x \wedge y = a \oplus b$. Now the winning probability of the CHSH game can be written as:

$$\Pr(win) = \sum_{s,t} \Pr_{xy}(s,t) \Pr(win|x = s, y = t), \tag{1}$$

which again implies that for $u, v, s, t \in \{0, 1\}$,

$$\Pr(win) = \sum_{s,t,u,v} \Pr_{xy}(s,t)(s \wedge t = u \oplus v) \Pr_{ab|xy}(a = u, b = v|x = s, y = t).$$

If the referee sends questions $x = 0, y = 0$, Alice and Bob win if they answer identically $a = 0, b = 0$ or $a = 1, b = 1$.

Then from Algorithm 1, the corresponding probability of winning (given $x = 0, y = 0$) is:

$\Pr(win|x = 0, y = 0) = |\langle 0| \otimes \langle \nu_0(\theta_0)| \Psi_{AB}\rangle|^2 + |\langle 1| \otimes \langle \nu_1(\theta_0)| \Psi_{AB}\rangle|^2 = \cos^2\theta_0$.

Similarly we have, $\Pr(win|x = 0, y = 1) = |\langle 0| \otimes \langle \nu_0(\theta_1)| \Psi_{AB}\rangle|^2 + |\langle 1| \otimes \langle \nu_1(\theta_1)| \Psi_{AB}\rangle|^2 = \cos^2\theta_1$, $\Pr(win|x = 1, y = 0) = |\langle 0_x| \otimes \langle \nu_0(\theta_0)| \Psi_{AB}\rangle|^2 + |\langle 1_x| \otimes \langle \nu_1(\theta_0)| \Psi_{AB}\rangle|^2 = \frac{1}{2}(1 + \sin 2\theta_0)$, $\Pr(win|x = 1, y = 1) = |\langle 0_x| \otimes \langle \nu_1(\theta_1)| \Psi_{AB}\rangle|^2 + |\langle 1_x| \otimes \langle \nu_0(\theta_1)| \Psi_{AB}\rangle|^2 = \frac{1}{2}(1 - \sin 2\theta_1)$.

Hence from Equation (1),

$$\begin{aligned} P(win) &= \frac{1}{4}(P(win|x = 0, y = 0) + P(win|x = 0, y = 1) \\ &\quad + P(win|x = 1, y = 0) + P(win|x = 1, y = 1)) \\ &= \frac{1}{4}\left[\cos^2\theta_0 + \cos^2\theta_1 + \frac{1}{2}(1 + \sin 2\theta_0) + \frac{1}{2}(1 - \sin 2\theta_1)\right]. \end{aligned}$$

This probability is maximum at $\left(\theta_0 = \frac{\pi}{8}, \theta_1 = \frac{15\pi}{8}\right)$ and the maximum value is approximately 0.85355.

3 Generalized version of the CHSH game

We generalize the well-known CHSH game to produce two types of new games. The first type of games are for 2-variables (i.e., each question has 2 options to answer). The other types of games are for 3-variables (i.e., each question has 3 options to answer).

Here also we assume that Alice and Bob are far away from each other and not able to communicate during the game. Before the game begins, they can communicate freely to discuss their strategy. During the game, they only communicate with the referee.

3.1 New games for 2-variables (Game-1)

Our new games are similar to the CHSH game. The only exception is in the winning condition. Here the winning condition is $f(x, y) = g_2(a, b)$, where f and g_2 are any two variable Boolean functions other than the constant functions (the subscript 2 in g_2 is for 2-variables). For 2 variables, there are $(2^2)^2 = 16$ possible Boolean functions. Among them 2 are constant functions. So we are playing this game with $14 \times 14 = 196$ pairs of function where in the CHSH game there is only one pair.

3.1.1 Rules of Game-1

For a fixed pair of two variable Boolean functions (f, g_2), we define Game-1 as follows:

- The referee chooses two independent random bits x and y uniformly (also called questions) and sends x to Alice and y to Bob, i.e., for all $s \in \{0, 1\}$, $t \in \{0, 1\}$, $\Pr(x = s, y = t) = \Pr_{xy}(s, t) = \frac{1}{4}$.
- Alice and Bob reply to referee with bits a and b, respectively.
- Referee calculates $f(x, y)$ and $g_2(a, b)$.
- Alice and Bob win if $f(x, y) = g_2(a, b)$.

3.1.2 Quantum strategy for Game-1

Alice and Bob follow the following strategy Algorithm 1 to play Game-1. Here also they share a maximally entangled state and choose measurement bases according to the referee's questions. They measure their qubits, and send their answers to the referee. Alice's choice of measurement basis only depends on referee's question. But for each pair (f, g_2), Bob chooses the basis for which they can achieve maximum winning probability. Bob's bases are dependent on the parameters θ_0 and θ_1. So for different pairs of functions (f, g_2), the values of θ_0 and θ_1 change. For example, CHSH game is a special case of Game-1, where $f = AND$, $g_2 = XOR$, and Bob chooses $\theta_0 = \frac{\pi}{8}$ and $\theta_1 = \frac{15\pi}{8}$.

3.1.3 Success probabilities of Game-1

We find the success probability of the game for each f and g_2 by using Equation (1), when the players follow the above strategy with changes in the chosen bases of Bob. Here Bob does not fix the value of θ_0 and θ_1. For different pairs of function (f, g_2), the value of the pair (θ_0, θ_1) changes as the expression of the winning probability changes.

Algorithm 1: Quantum Strategy for CHSH game and Game-1

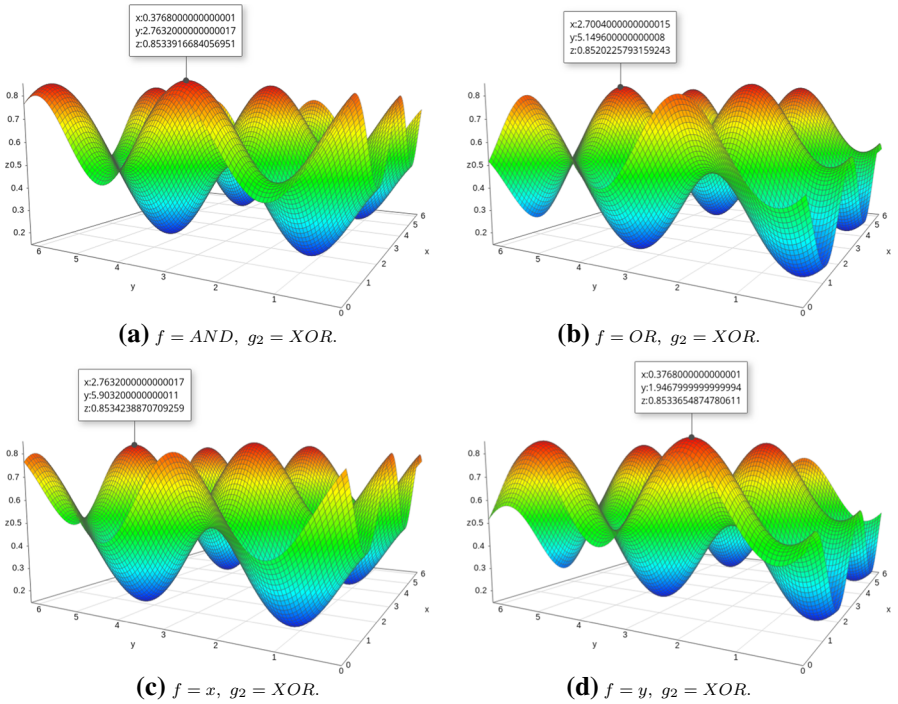
1. Before the game starts, Alice and Bob share $|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$
2. Alice takes the first qubit and Bob takes the second qubit
3. **Alice chooses:**
   - Standard basis $\{|0\rangle, |1\rangle\}$ if $x = 0$
   - Hadamard basis $\{|0_x\rangle, |1_x\rangle\}$ if $x = 1$, where $|0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
4. **Bob chooses:**
   Basis $\{|\nu_0(\theta_y)\rangle, |\nu_1(\theta_y)\rangle\}$ corresponding to $y = 0, 1$,
   where $|\nu_0(\theta_y)\rangle = \cos\theta_y |0\rangle + \sin\theta_y |1\rangle$, $|\nu_1(\theta_y)\rangle = \sin\theta_y |0\rangle - \cos\theta_y |1\rangle$, $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$
5. **Alice sends:**
   - $a = 0$ if $|0\rangle$ or $|0_x\rangle$
   - $a = 1$ otherwise
6. **Bob sends:**
   - $b = 0$ if Bob gets $|\nu_0(\theta_0)\rangle$ or $|\nu_0(\theta_1)\rangle$
   - $b = 1$ otherwise

Table 1 Success probabilities of Game-1 with any non-constant 2 variables Boolean functions f and g

LHS of winning condition $f(x, y)$	RHS of winning condition $g_2(a, b)$	Success probability	Number of such function pair (f, g_2)
Any non-constant f	XOR, XNOR	0.85	28
$f(x, y)$ contains one 0	$g_2(a, b)$ contains one 0	0.80	32
$f(x, y)$ contains one 1	$g_2(a, b)$ contains one 1	0.80	32
$f(x, y)$ contains two 0	$g_2(a, b)$ contains either exactly one 1 or 0	0.67	48
$f(x, y)$ contains one 1	$g_2(a, b)$ contains one 0	0.55	16
$f(x, y)$ contains one 0	$g_2(a, b)$ contains one 1	0.55	6
Any non-constant f	$g_2(a, b) = a, b, \bar{a}, \bar{b}$	0.5	56

For simplicity, we write an n-variable Boolean function as a 2^n-length binary vector consisting of the last column of the truth table in lexicographical order, e.g., for a two variable function, we write $f(x, y) = [f(0, 0), f(0, 1), f(1, 0), f(1, 1)]$ and $g_2(a, b) = [g_2(0, 0), g_2(0, 1), g_2(1, 0), g_2(1, 1)]$. Also LHS and RHS denote left-hand side and right-hand side, respectively.

The results are in the following Table 1. The first two columns of Table 1 represent the functions of inputs and outputs (i.e., $f(x, y)$ and $g_2(a, b)$), respectively, and corresponding success probabilities are given in third column. The number of such function pair (f, g_2) having same success probabilities are in the last column.



(a) $f = AND,\ g_2 = XOR.$ **(b)** $f = OR,\ g_2 = XOR.$

(c) $f = x,\ g_2 = XOR.$ **(d)** $f = y,\ g_2 = XOR.$

Fig. 1 Success probability graphs for four different cases of Game-1 with non-constant 2 variables Boolean functions f and g_2

3.1.4 Observation

From Table 1, we observe that the winning probability is maximum when $g_2(a, b) = a \oplus b$ and $a \odot b$, i.e., for any non-constant 2 variables Boolean function f, if $g_2 = XOR$ or $g_2 = XNOR$ then by playing the Game-1 we can win the game with probability 0.85.

The reason behind this is that the probability graph of these 28 cases are almost similar. To illustrate this, we show some probability graphs in Fig. 1. In these graphs, we plot θ_0 (x-axis) vs. θ_1(y-axis) vs. success probability expression (z-axis). From these graphs, we can see that for each case the success probabilities are periodic functions of (θ_0, θ_1) and achieve maximum value 0.85 at more than one points.

- The first graph in Figure 1(a) represents the success probability $\frac{1}{4}[1 + cos^2\theta_0 + cos^2\theta_1 + \frac{1}{2}sin2\theta_0 - \frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = AND,\ g_2 = XOR)$ and one of its maximum point is at $\left(\theta_0 = \frac{\pi}{8}, \theta_1 = \frac{15\pi}{8}\right)$.
- The second graph in Figure 1(b) represents the success probability $\frac{1}{4}[1 + cos^2\theta_0 + sin^2\theta_1 - \frac{1}{2}sin2\theta_0 - \frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = OR,\ g_2 = XOR)$ and one of its maximum point is at $\left(\theta_0 = \frac{7\pi}{8}, \theta_1 = \frac{5\pi}{8}\right)$.

- The third graph in Figure 1(c) represents the success probability $\frac{1}{4}[1 + cos^2\theta_0 + cos^2\theta_1 - \frac{1}{2}sin2\theta_0 - \frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = x,\ g_2 = XOR)$, where $f = x$ means $f(x, y) = x\ \forall\, x, y \in \{0, 1\}$, and one of its maximum point is at $\left(\theta_0 = \frac{7\pi}{8}, \theta_1 = \frac{7\pi}{8}\right)$.
- The fourth graph in Figure 1(d) represents the success probability $\frac{1}{4}[1 + cos^2\theta_0 + sin^2\theta_1 + \frac{1}{2}sin2\theta_0 - \frac{1}{2}sin2\theta_1]$ corresponding to the function pair $(f = y,\ g_2 = XOR)$, where $f = y$ means $f(x, y) = y\ \forall\, x, y \in \{0, 1\}$, and one of its maximum point is at $\left(\theta_0 = \frac{9\pi}{8}, \theta_1 = \frac{5\pi}{8}\right)$.

3.2 New games for 3-variables (Game-2)

In this game, there are two players, namely Alice and Bob (they are far away from each other and not able to communicate) and a referee. Let us define the sets $S = \{0, 1, 2\}$, $\mathcal{G} = \{g : S \times S \to \{0, 1\}\}$ and $\mathcal{F} = \{f : f\ is\ a\ 2\ variable\ Boolean function\}$.

3.2.1 Rules of Game-2

For a particular pair (f, g_3), where $f \in \mathcal{F}$ and $g_3 \in \mathcal{G}$ (the subscript 3 in g_3 is for 3-variables), we define Game-2 as follows:

- The referee chooses two independent random bits x and y uniformly (also called questions) and sends x to Alice and y to Bob. That is, for all $s \in \{0, 1\},\ t \in \{0, 1\},\ Pr(x = s, y = t) = P_{xy}(s, t) = \frac{1}{4}$.
- Alice and Bob send their answers a and b $(a, b \in \{0, 1, 2\})$ to the referee.
- Referee calculates $f(x, y)$ and $g_3(a, b)$.
- Alice and Bob win if $f(x, y) = g_3(a, b)$.

3.2.2 Quantum strategy for Game-2

Now let Alice and Bob play the game with the following strategy given in Algorithm 2. Before the game starts, they share a maximally entangled bipartite state: $|\Psi_{AB}\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B)$ in the Hilbert space $\mathbb{C}^3 \otimes \mathbb{C}^3$. According to the referee's questions, they choose measurement bases to measure their qubits and send their answers to the referee. Alice's choice of measurement basis only depends on referee's question. But for each pair (f, g_3), Bob choose the basis for which they can achieve maximum winning probability. Bob's bases are dependent on the parameters θ_0 and θ_1.

3.2.3 Example of Game-2

Let us take an example. Let $f(x, y) = x \wedge y$ and $g_3(a, b) = a\ Embedded\ XOR\ b$ (i.e., $g_3(a, b) = 0\ if\ a = b\ and\ g_3(a, b) = 1\ otherwise$). If we play the above game with these f and g_3, then the success probability is 0.76 at $\theta_0 = \frac{17\pi}{16}, \theta_1 = \frac{\pi}{16}$.

Algorithm 2: Quantum Strategy for Game-2

1. Before the game starts, Alice and Bob share
   $|\Psi_{AB}\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B)$
2. Alice takes the first qubit and Bob takes the second qubit
3. **Alice chooses:**
   - Standard basis $\{|0\rangle, |1\rangle, |2\rangle\}$ if $x = 0$
   - Fourier basis $\{|0_x\rangle, |1_x\rangle, |2_x\rangle\}$ if $x = 1$, where
     $|0_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$, $|1_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega|1\rangle + \omega^2|2\rangle)$,
     $|2_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2|1\rangle + \omega|2\rangle)$ and $\omega = e^{2\pi i/3}$
4. **Bob chooses:**
   - Basis $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$ if $y = 0$,
     $|\psi_0\rangle = \cos\theta_0|0\rangle + \sin\theta_0\cos\theta_1|1\rangle + \sin\theta_0\sin\theta_1|2\rangle$
     $|\psi_1\rangle = \sin\theta_0|0\rangle - \cos\theta_0\cos\theta_1|1\rangle - \cos\theta_0\sin\theta_1|2\rangle$
     $|\psi_2\rangle = \sin\theta_1|1\rangle + \cos\theta_1|2\rangle$ and
     $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$
   - Basis $\{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle\}$ if $y = 1$,
     $|\phi_0\rangle = \cos\theta_1|0\rangle + \sin\theta_1\cos\theta_0|1\rangle + \sin\theta_1\sin\theta_0|2\rangle$
     $|\phi_1\rangle = \sin\theta_1|0\rangle - \cos\theta_1\cos\theta_0|1\rangle - \cos\theta_1\sin\theta_0|2\rangle$
     $|\phi_2\rangle = \sin\theta_0|1\rangle + \cos\theta_0|2\rangle$ and
     $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$
5. **Alice sends:**
   - $a = 0$ if Alice gets $|0\rangle$ or $|0_x\rangle$
   - $a = 1$ if she gets $|1\rangle$ or $|1_x\rangle$
   - $a = 2$ otherwise
6. **Bob sends:**
   - $b = 0$ if Bob gets $|\psi_0\rangle$ or $|\phi_0\rangle$
   - $b = 1$ if he gets $|\psi_1\rangle$ or $|\phi_1\rangle$
   - $b = 2$ otherwise

3.2.4 Maximum winning probability

In this Game-2, the maximum winning probability is 0.86 only for 8 pairs of function (f, g_3).

Now the function pairs, with the highest winning probability and corresponding bases are shown in Table 2.

3.3 Equivalence classes

From the results of these two games, we observe that, if we introduce some equivalence relations to make partition of the set of data in each game result, then we will take only one element of each equivalence class to play these games. It will reduce the time and space complexity of these games. Also if some measurement setup will be unavailable then we can use any other setup from the same class to continue the games.

Table 2 Function pairs with maximum success probabilities of Game-2

f	g_3	θ_0	θ_1
[0, 1, 0, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	$33\pi/32$	$19\pi/32$
[0, 1, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	$29\pi/32$	$29\pi/32$
[0, 1, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	$29\pi/32$	$15\pi/32$
[0, 1, 1, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	$19\pi/32$	$33\pi/32$
[1, 0, 0, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	$19\pi/32$	$33\pi/32$
[1, 0, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	$29\pi/32$	$15\pi/32$
[1, 0, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	$15\pi/32$	$29\pi/32$
[1, 0, 1, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	$33\pi/32$	$19\pi/32$

Here we take three equivalence relations to make three different types of partitions of the results.

1. We can make an equivalence class of the bases of Bob for a fixed function pair (f, g_i), $(i = 2, 3)$, such that all elements of the same class give the same success probability.
   For simplicity, we only write the value of the pair (θ_1, θ_2) as a basis (i.e., we represent a basis as a point (θ_1, θ_2) in $\mathbb{R}^2$) in a class and we take the values in $radian$ (i.e., $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$) and as a multiple of $\frac{\pi}{32}$.
   For example, if we fix $f = AND$ and $g_2 = XOR$ in Game-1, then there are 8 equivalence classes of bases (up to 1 significant digit). Now in the previous example, if we consider the success probabilities up to 2 significant digits, then there are 4 elements in the class of highest winning probability 0.85 and the class is

$$\left\{\left(\frac{\pi}{8}, \frac{7\pi}{8}\right), \left(\frac{\pi}{8}, \frac{15\pi}{8}\right), \left(\frac{9\pi}{8}, \frac{7\pi}{8}\right), \left(\frac{9\pi}{8}, \frac{15\pi}{8}\right)\right\}.$$

   Again in Game-2, let $f = AND$ and $g_3 = Embedded\ XOR$ (i.e. $g_3(a, b) = 0\ if\ a = b\ and\ g_3(a, b) = 1\ otherwise$) , then there are 7 equivalence classes of bases (up to 1 significant digit). Now in the previous example, if we consider the success probabilities up to 2 significant digits, then there are 4 elements in the class of highest winning probability 0.76 and the class is

$$\left\{\left(\frac{33\pi}{32}, \frac{\pi}{32}\right), \left(\frac{33\pi}{32}, \frac{2\pi}{32}\right), \left(\frac{34\pi}{32}, \frac{\pi}{32}\right), \left(\frac{34\pi}{32}, \frac{2\pi}{32}\right)\right\}.$$

2. Secondly, we fix the bases of Bob and vary the function pairs to make the equivalence classes. Here also all the elements of the same class have the same winning probability.
   For example, in Game-1, if we fix $\left(\theta_0 = \frac{\pi}{8}, \theta_1 = \frac{15\pi}{8}\right)$, then ($f = [0, 0, 0, 1]$, $g_2 = [0, 1, 0, 1]$), ($f = [0, 0, 1, 0]$, $g_2 = [0, 1, 0, 1]$), ($f = [0, 0, 1, 1]$, $g_2 =$

[0, 1, 0, 1]), ($f = [0, 1, 1, 1]$, $g_2 = [0, 1, 0, 1]$), etc., all belong to the same class with success probability 0.5.

3. At last, we vary both function pairs and Bob's bases and the tuples which have the same winning probability that belongs to the same class. For example, in Game-2, each row of Table 2 have the same success probability 0.86 and thus they belong to the same class.

4 Dimensionality testing

We observe the winning probabilities of various cases in Game-1 and Game-2.

By using the above two games, we can make device-independent dimension distinguisher to distinguish between the states $|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$ and $|\Phi_{AB}\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B)$. For example,

- In Game-1, if we take $f(x, y) = x \wedge y$ and $g_2(a, b) = a \oplus b$ and $\theta_0 = \frac{\pi}{8}$, $\theta_1 = \frac{15\pi}{8}$, then the winning probability of this game is 0.85.
- In Game-2, if we take $f(x, y) = x \wedge y$ and $g_3 = Embedded\ XOR$ and $\theta_0 = \frac{\pi}{8}$, $\theta_1 = \frac{15\pi}{8}$, then winning probability of this game is 0.76.

So by playing these games and observing winning probabilities, we can easily distinguish between $|\Psi_{AB}\rangle$ and $|\Phi_{AB}\rangle$. In other words, we can say the dimension of the given maximally state is two or three.

We can think this whole process as a union of two black boxes. An initial black box is the state preparatory which prepares states of form either $|\Psi_{AB}\rangle$ or $|\Phi_{AB}\rangle$. the prepared state is then sent to a second black box, the measurement device. In this box, if the states are $|\Psi_{AB}\rangle$, it will follow the process of Game-1 and if the states are $|\Phi_{AB}\rangle$, it will follow the process of Game-2.

From the outputs of this measurement device, we will calculate the winning probability of the game played in this box and compare this probability with the success probabilities of Game-1 and Game-2. So we have a dimension distinguisher. The protocol is described in Algorithm 3.

Following the above process and by changing the function pairs in the games, we can find many distinguishers. For each, we use the function pair (f, g_3) in Game-2 and the function pair (f, g_2') in Game-1 (where, g_2' is the restriction of g_3 in 2 variables, i.e., $g_2'(a, b) = [g_3(0, 0), g_3(0, 1), g_3(1, 0), g_3(1, 1)]$). We divide the set of all distinguisher into 3 classes according to the winning probabilities of the games.

4.1 First class of distinguishers (D_1)

In this set, we put all the distinguishers where we choose function pairs (f, g_3) such that the function pair (f, g_2') has the highest winning probability in Game-1 (i.e., 0.85) which is greater than the winning probability of the corresponding Game-2.

Algorithm 3: Dimension distinguisher of maximally entangled state

Input: n number of maximally entangled bipartite state $|\Psi_{AB}\rangle$ in an Hilbert space $\mathbb{C}^d \times \mathbb{C}^d$ which is of the form $\sum_{j=1}^{d} \frac{1}{\sqrt{d}} |j\rangle \otimes |j\rangle$, where $\{|j\rangle\}$ is the standard basis of $\mathbb{C}^d$ and $d \in \{2, 3\}$ is fixed but unknown.

Output: The value of d.

1. For rounds $i \in \{1, \ldots, n\}$

   (a) Referee chooses $x_i \in \{0, 1\}$ and $y_i \in \{0, 1\}$ uniformly at random

   (b) If $x_i = 0$, Alice measures the first particle of the i-th entangled state in the standard basis $\{|0\rangle, |1\rangle, |2\rangle\}$
   • If $x_i = 1$, she measures that in the Fourier basis $\{|0_x\rangle, |1_x\rangle, |2_x\rangle\}$, where
   $|0_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$
   $|1_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega |1\rangle + \omega^2 |2\rangle)$
   $|2_x\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \omega^2 |1\rangle + \omega |2\rangle)$
   and $\omega = e^{2\pi i/3}$ (if $d = 2$, it will be the Hadamard basis)

   (c) Similarly,
   • If $y_i = 0$, Bob measures the second particle of the entangled state in $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$ basis , where
   $|\psi_0\rangle = \cos\theta_0 |0\rangle + \sin\theta_0 \cos\theta_1 |1\rangle + \sin\theta_0 \sin\theta_1 |2\rangle$
   $|\psi_1\rangle = \sin\theta_0 |0\rangle - \cos\theta_0 \cos\theta_1 |1\rangle - \cos\theta_0 \sin\theta_1 |2\rangle$
   $|\psi_2\rangle = \sin\theta_1 |1\rangle + \cos\theta_1 |2\rangle$
   $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$
   • If $y_i = 1$, he measures that in $\{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle\}$ basis, where
   $|\phi_0\rangle = \cos\theta_1 |0\rangle + \sin\theta_1 \cos\theta_0 |1\rangle + \sin\theta_1 \sin\theta_0 |2\rangle$
   $|\phi_1\rangle = \sin\theta_1 |0\rangle - \cos\theta_1 \cos\theta_0 |1\rangle - \cos\theta_1 \sin\theta_0 |2\rangle$
   $|\phi_2\rangle = \sin\theta_0 |1\rangle + \cos\theta_0 |2\rangle$
   $0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$

   (d) The output is recorded as $a_i(b_i) \in \{0, 1, 2\}$ for the first (second) particle. The encoding for $a_i(b_i)$ is as follows:
   • For the first particle of each pair, $a_i = j$ if the measurement result is $|j\rangle$ or $|j_x\rangle$
   • For the second particle of each pair,
   $b_i = 0$ if the measurement result is $|\psi_0\rangle$ or $|\phi_0\rangle$
   $b_i = 1$ if the measurement result is $|\psi_1\rangle$ or $|\phi_1\rangle$
   $b_i = 2$ if the measurement result is $|\psi_2\rangle$ or $|\phi_2\rangle$

   (e) For the test round i, define

$$Y_i = \begin{cases} 1 & \text{if } x_i \wedge y_i = g(a_i, b_i) \text{ where g=Embedded XOR} \\ 0 & \text{if otherwise} \end{cases}$$

2. Referee calculates $S = \frac{1}{n} \sum Y_i$
3. If $S \approx 0.85$, return $d = 2$ and if $S \approx 0.76$, return $d = 3$

If we choose $f = [0, 1, 0, 0]$, $g_3 = [0, 1, 1, 1, 0, 1, 1, 1, 0]$, thus $g_2' = [0, 1, 1, 0]$ (or $f = [0, 1, 1, 1]$, $g_3 = [1, 0, 0, 0, 1, 0, 0, 0, 1]$, thus $g_2' = [0, 1, 1, 0]$), then the winning probabilities of the Game-1 and Game-2 are 0.85 and 0.58. Therefore the difference of these probabilities is 0.27, which is quite good.

Table 3 Table for D_1

f	g_2'	g_3	W.P. if $d = 2$	W.P. if $d = 3$	Difference
[0, 0, 0, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 1, 1]	0.85	0.53	0.32
[0, 0, 0, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 1, 1, 1]	0.85	0.51	0.34
[0, 0, 0, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 1]	0.85	0.45	0.4
[0, 0, 1, 0]	[1, 0, 0, 1]	[1, 0, 0, 0, 1, 1, 1, 0, 1]	0.85	0.41	0.44
[0, 0, 1, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	0.85	0.39	0.46
[0, 1, 0, 0]	[0, 1, 1, 0]	[0, 1, 1, 1, 0, 1, 1, 1, 1]	0.85	0.42	0.43
[0, 1, 0, 1]	[0, 1, 1, 0]	[0, 1, 1, 1, 0, 1, 0, 1, 0]	0.85	0.46	0.39
[0, 1, 1, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 1, 0, 1, 0]	0.85	0.45	0.4
[1, 0, 0, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 0, 1, 0, 1]	0.85	0.53	0.32
[1, 0, 1, 0]	[1, 0, 0, 1]	[1, 0, 0, 0, 1, 0, 1, 0, 1]	0.85	0.46	0.39
[1, 0, 1, 1]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 1, 0, 0, 0]	0.85	0.44	0.41
[1, 1, 0, 0]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	0.85	0.39	0.46
[1, 1, 1, 0]	[0, 1, 1, 0]	[0, 1, 1, 1, 0, 0, 0, 0, 0]	0.85	0.41	0.44

∗W.P denotes winning probability

Table 4 Table for D_2

f	g_2'	g_3	W.P. if $d = 2$	W.P. if $d = 3$	Difference
[0, 1, 0, 0]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	0.46	0.86	0.4
[0, 1, 0, 0]	[1, 0, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	0.64	0.86	0.22
[0, 1, 1, 1]	[0, 1, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	0.63	0.86	0.23
[0, 1, 1, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	0.48	0.86	0.38
[1, 0, 0, 0]	[0, 1, 1, 0]	[0, 1, 0, 1, 0, 0, 0, 0, 1]	0.48	0.86	0.38
[1, 0, 0, 0]	[1, 0, 0, 0]	[1, 0, 0, 0, 0, 1, 0, 1, 0]	0.63	0.86	0.23
[1, 0, 1, 1]	[0, 1, 1, 1]	[0, 1, 1, 1, 1, 0, 1, 0, 1]	0.64	0.86	0.22
[1, 0, 1, 1]	[1, 0, 0, 1]	[1, 0, 1, 0, 1, 1, 1, 1, 0]	0.46	0.86	0.4

∗W.P denotes winning probability

There are many distinguishers in this class. We put some of them into the following Table 3. Here we take the winning probability for $d = 3$ at that point where the corresponding winning probability for $d = 2$ is maximum.

4.2 Second class of distinguishers (D_2)

In this set, we put all the distinguishers where we choose function pairs (f, g_3) such that it has the highest winning probability in Game-2 (i.e., 0.86) which is greater than the winning probability of corresponding Game-1 with function pair (f, g_2'). Here we take the winning probability for $d = 2$ at that point where the corresponding winning probability for $d = 3$ is maximum.

Table 5 Table for D_3

f	g_2'	g_3	W.P. if $d = 2$	W.P. if $d = 3$	Difference
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 0]	0.29	0.76	0.47
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 1]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 0]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 1]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 0, 0]	0.29	0.76	0.47
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 0, 1]	0.29	0.75	0.46
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 0]	0.29	0.77	0.48
[0, 0, 0, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 1]	0.29	0.76	0.47
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 0]	0.21	0.76	0.55
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 0, 1]	0.21	0.77	0.56
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 0]	0.21	0.77	0.56
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 1]	0.21	0.77	0.56
[0, 0, 1, 0]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 1]	0.21	0.76	0.55
[0, 0, 1, 1]	[1, 0, 1, 1]	[1, 0, 0, 1, 1, 0, 0, 1, 1]	0.36	0.81	0.45
[0, 0, 1, 1]	[1, 0, 1, 1]	[1, 0, 1, 1, 1, 0, 0, 1, 1]	0.36	0.84	0.48
[1, 1, 0, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 0]	0.36	0.84	0.48
[1, 1, 0, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 0]	0.36	0.81	0.45
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 0]	0.21	0.76	0.55
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 1]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 0]	0.21	0.75	0.54
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 1]	0.21	0.76	0.55
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 0]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 1]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 0]	0.21	0.77	0.56
[1, 1, 0, 1]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 1]	0.21	0.76	0.55
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 0]	0.29	0.76	0.47
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 0, 1]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 0]	0.29	0.75	0.46
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 0, 0, 0, 1, 1, 1, 1]	0.29	0.76	0.47
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 0]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 0, 1]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 0]	0.29	0.77	0.48
[1, 1, 1, 0]	[0, 1, 0, 0]	[0, 1, 1, 0, 0, 1, 1, 1, 1]	0.29	0.76	0.47

∗W.P denotes winning probability

For example, let $f = [0, 1, 0, 0]$, $g_3 = [1, 0, 0, 0, 0, 1, 0, 1, 0]$ then if $d = 2$ success probability is 0.80 and if $d = 3$ success probability is 0.86. We put all distinguishers in Table 4.

4.3 Third class of distinguishers (D_3)

Similarly, we can make dimension distinguisher using other function pairs for which the difference between the optimal winning probabilities of the two games is non-negligible. Here we take function pair (f, g_3) and corresponding pair (f, g_2') such that both the games with respective pairs do not achieve the highest winning probabilities. we put all these distinguishers in this set. The cardinality of this set depends on the difference value between winning probabilities.

Let (f, g_3) be a function pair and the highest winning probability of Game-2 with (f, g_3) being p_2 at point (s_2, t_2) and the same of Game-1 with (f, g_2') is p_1 at point (s_1, t_1). We compare p_1, p_2 and take the best (say, $p_1 > p_2$). Then we find the winning probability p of Game-2 at (s_1, t_1) and difference value $p_1 - p$. We make a list of these distinguishers for which the difference value is greater than 0.44 in Table 5.

5 Conclusion

Dimensionality of the states act as a resource in quantum information processing tasks. For many protocols, the performance as well as security depends on the particular value of the dimension. For this reason, dimensionality testing is very important. There have been several works on dimension witness. We take a different route by constructing dimension distinguishers based on our generalized version of the CHSH game. We demonstrate several classes of practical distinguishers between 2 and 3 dimensions.

References

1. Ekert, A.K.: Quantum cryptography based on Bells theorem. Phys. Rev. Lett. **67**, 661 (1991)
2. Bennett, C.H., Wiesner, S.J.: Communication via one-and two-particle operators on Einstein–Podolsky–Rosen states. Phys. Rev. Lett. **69**(20), 2881 (1992)
3. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895 (1993)
4. Bose, S., Vedral, V., Knight, P.L.: Multiparticle generalization of entanglement swapping. Phys. Rev. A **57**(2), 822 (1998)
5. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. Rev. Mod. Phys. **81**(2), 865 (2009)
6. Einstein, A., Podolsky, B., Rosen, N.: Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**(10), 777 (1935)
7. Bell, J.S.: On the einstein podolsky rosen paradox. Phys. Phys. Fiz. **1**(3), 195 (1964)
8. Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A.: Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. **23**(15), 880 (1969)
9. Cirel'son, B.S.: Quantum generalizations of Bell's inequality. Lett. Math. Phys. **4**(2), 93–100 (1980)
10. Grangier, P., Roger, G., Aspect, A.: Experimental evidence for a photon anticorrelation effect on a beam splitter: a new light on single-photon interferences. Europhys. Lett. **1**(4), 173 (1986)
11. Popescu, S., Rohrlich, D.: Quantum nonlocality as an axiom. Found. Phys. **24**(3), 379–385 (1994)
12. http://northala.net/qit/handouts/2016-Handout2.pdf
13. https://sergworks.wordpress.com/2016/10/26/chsh-game-in-detail/
14. Buhrman, H., Massar, S.: Causality and Tsirelson's bounds. Phys. Rev. A **72**(5), 052103 (2005)
15. Toner, B.: Monogamy of non-local quantum correlations. Proc. R. Soc. A Math. Phys. Eng. Sci. **465**(2101), 59–69 (2008)

16. Pawowski, M.: Security proof for cryptographic protocols based only on the monogamy of Bells inequality violations. Phys. Rev. A **82**(3), 032313 (2010)
17. Reichardt, B.W., Unger, F., Vazirani, U.: Classical command of quantum systems. Nature **496**(7446), 456 (2013)
18. Brunner, N., Linden, N.: Connection between Bell nonlocality and Bayesian game theory. Nat. Commun. **4**, 2057 (2013)
19. Bavarian, M., Shor, P. W.: Information causality, Szemerdi–Trotter and algebraic variants of CHSH. In: Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ACM, pp 123–132 (2015)
20. Brunner, N., Pironio, S., Acin, A., Gisin, N., Méthot, A.A., Scarani, V.: Testing the dimension of Hilbert spaces. Phys. Rev. Lett. **100**(21), 210503 (2008)
21. Pál, K.F., Vértesi, T.: Efficiency of higher-dimensional Hilbert spaces for the violation of Bell inequalities. Phys. Rev. A **77**(4), 042105 (2008)
22. Pérez-García, D., Wolf, M.M., Palazuelos, C., Villanueva, I., Junge, M.: Unbounded violation of tripartite Bell inequalities. Commun. Math. Phys. **279**(2), 455–486 (2008)
23. Vértesi, T., Pironio, S., Brunner, N.: Closing the detection loophole in Bell experiments using qudits. Phys. Rev. Lett. **104**(6), 060401 (2010)
24. Vértesi, T., Pál, K.F.: Generalized Clauser-Horne-Shimony-Holt inequalities maximally violated by higher-dimensional systems. Phys. Rev. A **77**(4), 042106 (2008)
25. Junge, M., Palazuelos, C., Pérez-García, D., Villanueva, I., Wolf, M.M.: Operator space theory: a natural framework for Bell inequalities. Phys. Rev. Lett. **104**(17), 170405 (2010)
26. Briët, J., Buhrman, H., Toner, B.: A generalized Grothendieck inequality and nonlocal correlations that require high entanglement. Commun. Math. Phys. **305**(3), 827–843 (2011)
27. Wehner, S., Christandl, M., Doherty, A.C.: Lower bound on the dimension of a quantum system given measured data. Phys. Rev. A **78**(6), 062112 (2008)
28. Gallego, R., Brunner, N., Hadley, C., Acín, A.: Device-independent tests of classical and quantum dimensions. Phys. Rev. Lett. **105**(23), 230501 (2010)
29. Junge, M., Palazuelos, C.: Large violation of Bell inequalities with low entanglement. Commun. Math. Phys. **306**(3), 695 (2011)
30. Ahrens, J., Badziag, P., Cabello, A., Bourennane, M.: Experimental device-independent tests of classical and quantum dimensions. Nat. Phys. **8**(8), 592 (2012)
31. Hendrych, M., Gallego, R., Mičda, M., Brunner, N., Acín, A., Torres, J.P.: Experimental estimation of the dimension of classical and quantum systems. Nat. Phys. **8**(8), 588 (2012)
32. Ahrens, J., Badziag, P., Cabello, A., Bourennane, M.: Experimental device-independent tests of classical and quantum dimensions. Nat. Phys. **8**(8), 592 (2012)
33. Brunner, N., Navascués, M., Vértesi, T.: Dimension witnesses and quantum state discrimination. Phys. Rev. Lett. **110**(15), 150501 (2013)
34. Bowles, J., Quintino, M.T., Brunner, N.: Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. Phys. Rev. Lett. **112**(14), 140407 (2014)
35. Maitra, A., Adhikari, B., Adhikari, S.: Proposal for dimensionality testing in QPQ. Quantum Inf. Comput. **18**(13&14), 1125–1142 (2018)
36. Paul, G., Ray, S.: On data complexity of distinguishing attacks versus message recovery attacks on stream ciphers. Des. Codes Cryptogr. **86**, 1211–1247 (2018)
37. Basak, J., Maitra, S.: ClauserHorneShimonyHolt versus three-party pseudo-telepathy: on the optimal number of samples in device-independent quantum private query. Quantum Inf. Process **17**(4), 77 (2018)