# Greenberger-Horne-Zeilinger-like proof of Bell's theorem involving observers who do not share a reference frame

Adán Cabello*

*Departamento de Física Aplicada II, Universidad de Sevilla, 41012 Sevilla, Spain*

(Received 12 June 2003; published 9 October 2003)

Vaidman described how a team of three players, each of them isolated in a remote booth, could use a three-qubit Greenberger-Horne-Zeilinger state to always win a game which would be impossible to always win without quantum resources. However, Vaidman's method requires all three players to share a common reference frame; it does not work if the adversary is allowed to disorientate one player. Here we show how to always win the game, even if the players do not share any reference frame. The introduced method uses a 12-qubit state which is invariant under any transformation $R_a \otimes R_b \otimes R_c$ (where $R_a = U_a \otimes U_a \otimes U_a \otimes U_a$, where $U_j$ is a unitary operation on a single qubit) and requires only single-qubit measurements. A number of further applications of this 12-qubit state are described.

DOI: 10.1103/PhysRevA.68.042104 PACS number(s): 03.65.Ud, 03.65.Ta

## I. INTRODUCTION

In 1991, after months of patient "work" and based on a study of 20 000 events, a gang of players reached an amazing conclusion: in eight roulette wheels of the Gran Casino of Madrid, six numbers (1 and its two neighbors, 20 and 33, and the opposite number in the roulette wheel, 4, and its two neighbors, 19 and 21) occurred with an unexpectedly high frequency (assuming that each of the 37 numbers of the roulette wheel appears with the same frequency), while four numbers (11, 12, 28, and 36) rarely occurred. The gang won a large amount of money by betting in these roulette wheels. The casino never realized where the problem was, never understood the "method" used by the gang but, after many attempts, found its own method to defeat the gang: the casino started to regularly exchange the pieces of the roulette wheels and switch the numbers' positions. This altered the roulette wheels' original "defects" and the gang stopped winning [1]. The moral is that any winning strategy usually has an antidote.

In 1999, Vaidman [2] converted Mermin's [3,4] version of the proof of Bell's theorem without inequalities discovered by Greenberger, Horne, and Zeilinger (GHZ) [5–7] into a game involving a team (a gang) of three players, each of them completely isolated in a booth, and an opponent (a casino). Under some assumptions, and using only classical resources, the maximum probability for the team to win Vaidman's game is 75% (thus a casino gets profit by exploiting the remaining 25%). Thanks to the fact that rules of the game do not forbid the players to share qubits prepared in some entangled state, there is a method which allows them to always win the game. However, there is a simple manipulation that nullifies the quantum advantage. A hidden assumption of the method is that all three players share a common reference frame. If the casino disorientates one of the players so that all three of them do not share a reference frame, then the advantage of the method is lost. The term "unspeakable information" was coined by Peres and Scudo [8] to designate information that cannot be represented by a sequence of discrete symbols, such as a direction in space or a reference frame. In this paper we show that there is a method to always win Vaidman's game without it being necessary that the players share unspeakable information.

In Sec. II we review the rules of Vaidman's game and the original quantum method for always winning. In Sec. III we propose a quantum method for always winning, even if the players do not share any reference frame. This method requires more qubits, and thus one might think that it must require collective measurements on several qubits, instead of single-qubit measurements, as in the original method; in Sec. IV we shall see that this is not the case. In Sec. V we show other applications of the method.

## II. VAIDMAN'S GAME

### A. Rules

Vaidman proposed the following game [2]. Consider a team of three players, who are allowed to agree on a common strategy and make any preparation before they are taken to three remote and isolated booths. Then, each player is asked one of the two possible questions: "What is $Z$?" or "What is $X$?" Each player must give an answer which is limited to one of only two possibilities: "0" or "1." One of the rules of the game is that either all three players are asked the $Z$ question or only one player is asked the $Z$ question and the other two are asked the $X$ question. The team wins if the number of 0 answers is odd (one or three) in the case of three $Z$ questions, and is even (zero or two) in the case of one $Z$ and two $X$ questions.

Assuming that the four possible combinations of questions (i.e., $Z_1,Z_2,Z_3$; $Z_1,X_2,X_3$; $X_1,Z_2,X_3$; and $X_1,X_2,Z_3$) are asked with the same frequency, no classical protocol allows the players to win the game in more than 75% of the runs. For instance, a simple strategy that allows them to win in 75% of the runs is that each player always answers 1 to the $Z$ question and 0 to the $X$ question. However, quantum mechanics provides a method to always win the game.

*Electronic address: adan@us.es

### B. GHZ-assisted quantum always winning strategy

The method for always winning is the following. Before entering the isolated booths, the players prepare a large number of three-qubit systems in the GHZ state [3–7,9]:

$$|\mathrm{GHZ}\rangle=\frac{1}{\sqrt{2}}(|y_0,y_0,y_0\rangle+|y_1,y_1,y_1\rangle). \tag{1}$$

Here $|y_0,y_0,y_0\rangle=|y_0\rangle\otimes|y_0\rangle\otimes|y_0\rangle$, where $|y_0\rangle=(1/\sqrt{2})\times(|z_0\rangle+i|z_1\rangle)$ and $|y_1\rangle=(1/\sqrt{2})(|z_0\rangle-i|z_1\rangle)$, $|z_0\rangle=\binom{1}{0}$ and $|z_1\rangle=\binom{0}{1}$. Then, for each three-qubit system, each of the players takes one of the qubits with him. In case a player is asked "What is $Z$?," he performs a measurement on his qubit of the observable represented by

$$Z=|z_0\rangle\langle z_0|-|z_1\rangle\langle z_1|, \tag{2}$$

and gives the answer 0, if the outcome corresponds to $|z_0\rangle$, or the answer 1, if the outcome corresponds to $|z_1\rangle$.

In case a player is asked "What is $X$?," he performs a measurement of the observable represented by

$$X=|x_0\rangle\langle x_0|-|x_1\rangle\langle x_1|, \tag{3}$$

where $|x_0\rangle=(1/\sqrt{2})(|z_0\rangle+|z_1\rangle)$ and $|x_1\rangle=(1/\sqrt{2})(|z_0\rangle-|z_1\rangle)$, and gives the answer 0, if the outcome corresponds to $|x_0\rangle$, or the answer 1, if the outcome corresponds to $|x_1\rangle$.

The protocol described above allows the team to always win the game, because the state defined in Eq. (1) can also be expressed in the following four forms:

$$|\mathrm{GHZ}\rangle=\tfrac{1}{2}(|z_0,z_0,z_0\rangle-|z_0,z_1,z_1\rangle-|z_1,z_0,z_1\rangle-|z_1,z_1,z_0\rangle) \tag{4}$$

$$=\tfrac{1}{2}(|z_0,x_0,x_1\rangle+|z_0,x_1,x_0\rangle-|z_1,x_0,x_0\rangle+|z_1,x_1,x_1\rangle) \tag{5}$$

$$=\tfrac{1}{2}(|x_0,z_0,x_1\rangle-|x_0,z_1,x_0\rangle+|x_1,z_0,x_0\rangle+|x_1,z_1,x_1\rangle) \tag{6}$$

$$=\tfrac{1}{2}(-|x_0,x_0,z_1\rangle+|x_0,x_1,z_0\rangle+|x_1,x_0,z_0\rangle+|x_1,x_1,z_1\rangle). \tag{7}$$

It can be inferred from Eq. (4) that if all players measure $Z$, then either all of them will obtain $z_0$, or one will obtain $z_0$ and the other two will obtain $z_1$. Analogously, it can be inferred from Eqs. (5)–(7) that, if one player measures $Z$ and the other two measure $X$, then either all of them will obtain 1, or one will obtain 1 and the other two will obtain 0.

## III. QUANTUM ALWAYS WINNING STRATEGY WITHOUT UNSPEAKABLE INFORMATION

The method described above has one drawback that the adversary could use to keep the players from always winning. If the qubits are spin states of spin-$\frac{1}{2}$ particles, then the observables $Z$ and $X$ can be identified, respectively, with the spin components along two orthogonal directions $z$ and $x$. Such directions are determined by the preparation of the GHZ state (1). This method requires all players to share the directions $z$ and $x$ for the duration of the game. However, if the opponent finds a way to confuse one of them, then the local measurements performed by the players will not be adequately correlated and thus the advantage provided by the GHZ state is lost.

Fortunately, there is a method which is still valid even if the players do not share two directions. Now, before entering the booths, the players prepare a large number of 12-qubit systems in the state

$$|\Psi\rangle=\frac{1}{\sqrt{2}}(|\eta_0,\eta_0,\eta_0\rangle+|\eta_1,\eta_1,\eta_1\rangle), \tag{8}$$

where $|\eta_0\rangle=(1/\sqrt{2})(|\phi_0\rangle+i|\phi_1\rangle)$ and $|\eta_1\rangle=(1/\sqrt{2})(|\phi_0\rangle-i|\phi_1\rangle)$, where $|\phi_0\rangle$ and $|\phi_1\rangle$ are the four-qubit states

$$|\phi_0\rangle=\frac{1}{2}(|z_0,z_1,z_0,z_1\rangle-|z_0,z_1,z_1,z_0\rangle-|z_1,z_0,z_0,z_1\rangle+|z_1,z_0,z_1,z_0\rangle), \tag{9}$$

$$|\phi_1\rangle=\frac{1}{2\sqrt{3}}(2|z_0,z_0,z_1,z_1\rangle-|z_0,z_1,z_0,z_1\rangle-|z_0,z_1,z_1,z_0\rangle-|z_1,z_0,z_0,z_1\rangle-|z_1,z_0,z_1,z_0\rangle+2|z_1,z_1,z_0,z_0\rangle), \tag{10}$$

introduced by Kempe *et al.* [10] in the context of decoherence-free fault-tolerant universal quantum computation [11,12], and recently obtained experimentally using parametric down-converted polarization-entangled photons [13].

Then, for each 12-qubit system, the first player takes the first *four* qubits with him, the second player takes the next four qubits, and the third player takes the last four qubits. In case a player is asked "What is $Z$?," he performs on his four qubits a measurement of the observable represented by

$$\mathcal{Z}=|\phi_0\rangle\langle\phi_0|-|\phi_1\rangle\langle\phi_1|. \tag{11}$$

The observable $\mathcal{Z}$ has *three* possible outcomes (corresponding to its three eigenvalues $-1$, 0, and 1). However, if the qubits have been prepared in the state $|\Psi\rangle$ given in Eq. (8), then only two outcomes can occur (those corresponding to the eigenvalues $-1$ and 1). Measuring the observable $\mathcal{Z}$ on a system prepared in the state $|\Psi\rangle$ is then equivalent to reliably discriminating between the states $|\phi_0\rangle$ and $|\phi_1\rangle$. The player gives the answer 0, if the outcome corresponds to $|\phi_0\rangle$, and the answer 1, if the outcome corresponds to $|\phi_1\rangle$.

In case a player is asked "What is $X$?," he performs a measurement of the observable represented by

$$\mathcal{X}=|\psi_0\rangle\langle\psi_0|-|\psi_1\rangle\langle\psi_1|, \tag{12}$$

where

$$|\psi_0\rangle=\frac{1}{\sqrt{2}}(|\phi_0\rangle+|\phi_1\rangle), \tag{13}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\phi_0\rangle - |\phi_1\rangle). \tag{14}$$

Measuring $\mathcal{X}$ on a system prepared in the state $|\Psi\rangle$ is equivalent to reliably discriminating between $|\psi_0\rangle$ and $|\psi_1\rangle$. The player gives the answer 0, if the outcome corresponds to $|\psi_0\rangle$, or the answer 1, if the outcome corresponds to $|\psi_1\rangle$.

The state $|\Psi\rangle$ can be expressed in the following four forms:

$$\begin{aligned}|\Psi\rangle = \tfrac{1}{2}(&|\phi_0,\phi_0,\phi_0\rangle - |\phi_0,\phi_1,\phi_1\rangle - |\phi_1,\phi_0,\phi_1\rangle \\ &- |\phi_1,\phi_1,\phi_0\rangle)\end{aligned} \tag{15}$$

$$\begin{aligned}= \tfrac{1}{2}(&|\phi_0,\psi_0,\psi_1\rangle + |\phi_0,\psi_1,\psi_0\rangle - |\phi_1,\psi_0,\psi_0\rangle \\ &+ |\phi_1,\psi_1,\psi_1\rangle)\end{aligned} \tag{16}$$

$$\begin{aligned}= \tfrac{1}{2}(&|\psi_0,\phi_0,\psi_1\rangle - |\psi_0,\phi_1,\psi_0\rangle + |\psi_1,\phi_0,\psi_0\rangle \\ &+ |\psi_1,\phi_1,\psi_1\rangle)\end{aligned} \tag{17}$$

$$\begin{aligned}= \tfrac{1}{2}(&-|\psi_0,\psi_0,\phi_1\rangle + |\psi_0,\psi_1,\phi_0\rangle + |\psi_1,\psi_0,\phi_0\rangle \\ &+ |\psi_1,\psi_1,\phi_1\rangle).\end{aligned} \tag{18}$$

From Eq. (15), it can be inferred that if the three players perform measurements to discriminate between $|\phi_0\rangle$ and $|\phi_1\rangle$, then they will always obtain an odd number of states $|\phi_0\rangle$. From Eqs. (16) to (18), it can be inferred that if two players perform measurements to discriminate between $|\psi_0\rangle$ and $|\psi_1\rangle$, and the third performs measurements to discriminate between $|\phi_0\rangle$ and $|\phi_1\rangle$, then they will always obtain an odd number of states $|\psi_1\rangle$ and $|\phi_1\rangle$.

For our purposes, the fundamental property of the state $|\Psi\rangle$ is that it is invariant under any transformation $R_a \otimes R_b \otimes R_c$ (where $R_a = U_a \otimes U_a \otimes U_a \otimes U_a$, where $U_j$ is a unitary operation on a single qubit). This property derives from the fact that $|\phi_0\rangle$ and $|\phi_1\rangle$ and any linear combination thereof (such as $|\psi_0\rangle$ and $|\psi_1\rangle$) are invariant under the tensor product of four equal unitary operators, $U_j \otimes U_j \otimes U_j \otimes U_j$. This means that the state $|\Psi\rangle$ is invariant under local rotations, and the local observables $\mathcal{Z}$ and $\mathcal{X}$ are invariant under $U_j \otimes U_j \otimes U_j \otimes U_j$ and thus under rotations of the local setups [14]. Therefore, expressions (15)–(18) remain unchanged after local rotations. This implies that even if the adversary disorientates one or more players, the outcomes of the local measurements still possess the desired correlations, because the involved local measurements are rotationally invariant.

## IV. MEASURING THE OBSERVABLES BY USING SINGLE-QUBIT MEASUREMENTS

One might think that measuring $\mathcal{Z}$ (i.e., distinguishing between $|\phi_0\rangle$ and $|\phi_1\rangle$) and $\mathcal{X}$ (i.e., distinguishing between $|\psi_0\rangle$ and $|\psi_1\rangle$) could require collective measurements on each player's four qubits. However, as in the original method, only single-qubit measurements are needed.

### A. Distinguishing between $|\phi_0\rangle$ and $|\phi_1\rangle$

The states $|\phi_0\rangle$ and $|\phi_1\rangle$ are reliably distinguishable using single-qubit measurements because they can be expressed as

$$\begin{aligned}|\phi_0\rangle = \frac{1}{2}(&-|z_0,z_1,x_0,x_1\rangle + |z_0,z_1,x_1,x_0\rangle + |z_1,z_0,x_0,x_1\rangle \\ &- |z_1,z_0,x_1,x_0\rangle),\end{aligned} \tag{19}$$

$$\begin{aligned}|\phi_1\rangle = \frac{1}{2\sqrt{3}}(&|z_0,z_0,x_0,x_0\rangle - |z_0,z_0,x_0,x_1\rangle - |z_0,z_0,x_1,x_0\rangle \\ &+ |z_0,z_0,x_1,x_1\rangle - |z_0,z_1,x_0,x_0\rangle + |z_0,z_1,x_1,x_1\rangle \\ &- |z_1,z_0,x_0,x_0\rangle + |z_1,z_0,x_1,x_1\rangle + |z_1,z_1,x_0,x_0\rangle \\ &+ |z_1,z_1,x_0,x_1\rangle + |z_1,z_1,x_1,x_0\rangle + |z_1,z_1,x_1,x_1\rangle).\end{aligned} \tag{20}$$

Therefore, if the local measurements are $Z_1$ (i.e., the component along the $z$ direction of the first qubit), $Z_2$ (i.e., the component along the $z$ direction of the second qubit), $X_3$ (i.e., the component along the $x$ direction of the third qubit), and $X_4$ (i.e., the component along the $x$ direction of the fourth qubit) then, among the 16 possible outcomes, 4 occur (with equal probability) only if the qubits were in the state $|\phi_0\rangle$, and the other 12 outcomes occur (with equal probability) only if the qubits were in the state $|\phi_1\rangle$. Note that now $z$ and $x$ are not fixed directions, but any two orthogonal directions instead. This scheme to distinguish between $|\phi_0\rangle$ and $|\phi_1\rangle$ using only single-qubit measurements has recently been experimentally implemented [13].

### B. Distinguishing between $|\psi_0\rangle$ and $|\psi_1\rangle$

The states $|\psi_0\rangle$ and $|\psi_1\rangle$ are not distinguishable using *fixed* single-qubit measurements. However, any two orthogonal states are distinguishable by single-qubit measurements *assisted by classical communication* [15]. This means that there is a *sequence* of single-qubit measurements which allows us to reliably distinguish between $|\psi_0\rangle$ and $|\psi_1\rangle$. In this sequence, what is measured on one qubit could depend on the result of a prior measurement on a different qubit. A sequence of single-qubit measurements which allows us to reliably distinguish between $|\psi_0\rangle$ and $|\psi_1\rangle$ follows from the fact that these states can be expressed as

$$\begin{aligned}|\psi_0\rangle = \alpha|z_0,x_0,a_0,c_0\rangle &+ \beta|z_0,x_0,a_1,d_1\rangle + \alpha|z_0,x_1,b_0,e_0\rangle \\ &+ \beta|z_0,x_1,b_1,f_1\rangle + \beta|z_1,x_0,b_0,f_0\rangle \\ &+ \alpha|z_1,x_0,b_1,e_1\rangle - \beta|z_1,x_1,a_0,d_0\rangle \\ &+ \alpha|z_1,x_1,a_1,c_1\rangle,\end{aligned} \tag{21}$$

$$\begin{aligned}|\psi_1\rangle=&\beta|z_0,x_0,a_0,c_1\rangle+\alpha|z_0,x_0,a_1,d_0\rangle+\beta|z_0,x_1,b_0,e_1\rangle\\&-\alpha|z_0,x_1,b_1,f_0\rangle+\alpha|z_1,x_0,b_0,f_1\rangle\\&-\beta|z_1,x_0,b_1,e_0\rangle+\alpha|z_1,x_1,a_0,d_1\rangle\\&-\beta|z_1,x_1,a_1,c_0\rangle,\end{aligned} \tag{22}$$

where

$$\alpha=\frac{\sqrt{3+\sqrt{6}}}{2\sqrt{6}}, \tag{23}$$

$$\beta=\frac{\sqrt{3-\sqrt{6}}}{2\sqrt{6}}, \tag{24}$$

and

$$|a_0\rangle=p|z_0\rangle+q|z_1\rangle, \quad |a_1\rangle=q|z_0\rangle-p|z_1\rangle, \tag{25}$$

$$|b_0\rangle=-p|z_0\rangle+q|z_1\rangle, \quad |b_1\rangle=q|z_0\rangle+p|z_1\rangle, \tag{26}$$

$$|c_0\rangle=-r|z_0\rangle+s|z_1\rangle, \quad |c_1\rangle=-s|z_0\rangle-r|z_1\rangle, \tag{27}$$

$$|d_0\rangle=t|z_0\rangle+u|z_1\rangle, \quad |d_1\rangle=u|z_0\rangle-t|z_1\rangle, \tag{28}$$

$$|e_0\rangle=r|z_0\rangle+s|z_1\rangle, \quad |e_1\rangle=s|z_0\rangle-r|z_1\rangle, \tag{29}$$

$$|f_0\rangle=-t|z_0\rangle+u|z_1\rangle, \quad |f_1\rangle=u|z_0\rangle+t|z_1\rangle, \tag{30}$$

where

$$p=\frac{\sqrt{2-\sqrt{2}}}{2}, \tag{31}$$

$$q=\frac{\sqrt{2+\sqrt{2}}}{2}, \tag{32}$$

$$r=\frac{(3+\sqrt{3})q}{12\alpha}, \tag{33}$$

$$s=\frac{(3-\sqrt{3})q}{12\beta}, \tag{34}$$

$$t=\frac{(3-\sqrt{3})p}{12\alpha}, \tag{35}$$

$$u=\frac{(3+\sqrt{3})p}{12\beta}. \tag{36}$$

Note that, for instance, the state $|b_0\rangle$ is *not* orthogonal to $|a_0\rangle$ or $|a_1\rangle$. The comparison between expressions (21) and (22) leads us to a simple protocol for reliably distinguishing between $|\psi_0\rangle$ and $|\psi_1\rangle$ using a sequence of single-qubit measurements. This protocol is shown in Fig. 1.

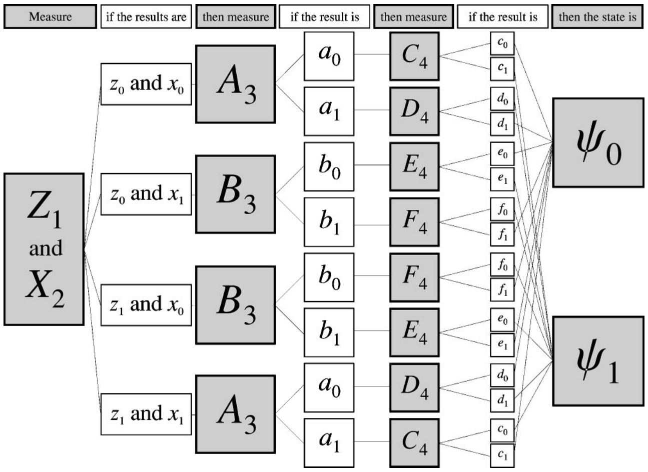

FIG. 1. Protocol for reliably distinguishing $|\psi_0\rangle$ and $|\psi_1\rangle$ using a sequence of single-qubit measurements. Example: first, measure $Z$ on qubit 1 and $X$ on qubit 2. If the results are, respectively, $z_0$ and $x_1$, then measure the observable represented by $B=|b_0\rangle\langle b_0|-|b_1\rangle\langle b_1|$ on qubit 3. If the result is $b_0$, then measure the observable $E=|e_0\rangle\langle e_0|-|e_1\rangle\langle e_1|$ on qubit 4. If the result is $e_1$, then the state is $|\psi_1\rangle$.

## V. OTHER APPLICATIONS

### A. No-hidden-variables theorems

Vaidman's aim was to reformulate the GHZ proof of Bell's theorem into a game "which can convert laymen into admirers of quantum theory" by showing its "miraculous power" [2]. One obvious application of the method for always winning Vaidman's game introduced in this paper is thus to prove Bell's theorem without inequalities when the local observers do not share any reference frame. According to Eqs. (15)–(18), one can predict with certainty the value of either $\mathcal{Z}_j$ or $\mathcal{X}_j$ (with $j=1,2,3$) from the results of spacelike separated measurements on the other two four-qubit systems. Therefore, for any $j$, $\mathcal{Z}_j$ and $\mathcal{X}_j$ can be considered "elements of reality," as defined by Einstein, Podolsky, and Rosen [16]. However, it is impossible to assign predefined values, either 0 or 1, to the six observables $\mathcal{Z}_j$ and $\mathcal{X}_j$ satisfying all predictions given by Eqs. (15)–(18).

This proof is of interest, since it shows that a perfect alignment between the source of entangled states and the local detectors does not play a fundamental role in Bell's theorem. For instance, in 1988 Yuval Ne'eman argued that the answer to the puzzle posed by Bell's theorem was to be found in the implicit assumption that the detectors were aligned. Ne'eman apparently believed that the two detectors were connected through the space-time affine connection of general relativity [17]. A proof of Bell's theorem without inequalities and without alignments involving two observers, eight-qubit states, and only fixed single-qubit measurements (i.e., without requiring a protocol like the one in Fig. 1) has been introduced in Ref. [18]. The interest of the proof of Bell's theorem without inequalities for the state $|\Psi\rangle$, given in Eq. (8), and the local measurements of $\mathcal{Z}$ and $\mathcal{X}$, defined respectively in Eqs. (11) and (12), is that such a proof is valid for 100% of the events prepared in the state $|\Psi\rangle$, instead of only for a small (8%) subset of the events in Ref. [18].

Other interesting application of the state $|\Psi\rangle$ and the local observables $\mathcal{Z}$ and $\mathcal{X}$ is the Kochen-Specker (KS) theorem of impossibility of noncontextual hidden variables in quantum mechanics [19]. Mermin showed how the GHZ proof of Bell's theorem could be converted into a proof of the KS theorem [20,21]. Analogously, the proof of Bell's theorem using $|\Psi\rangle$, $\mathcal{Z}$, and $\mathcal{X}$ could be converted into a (subspace-dependent) proof of the KS theorem, valid even for measurements along imperfectly defined directions. This is of interest, because it sheds some extra light on a recent debate about whether or not the KS theorem is still valid when ideal measurements are replaced by imperfect measurements [22–30].

### B. Reducing the communication complexity with prior entanglement

Vaidman's game can also be seen as a scenario in which the communication complexity of a certain task can be reduced if the players are allowed to share some prior entangled state. In Vaidman's game the task is to always win the game. Without quantum resources, this task requires at least one of the players to send 1 bit to other player after the question ($Z$ or $X$) has been posed to him. However, if they initially share a GHZ state, the task does not require any transmission of classical information between the players.

A similar example of reduction of the communication complexity needed for a task if the parties share a GHZ state was discovered by Cleve and Buhrman [31], reformulated by Buhrman *et al.* [32], and attractively presented by Steane and van Dam [33] as follows: a secret integer number $n_A+n_B+n_C$ of apples, where $n_j=0, \frac{1}{2}, 1$, or $\frac{3}{2}$, is distributed among three players, Alice, Bob, and Charlie, of the same team. Each of them is in an isolated booth. The team wins if one of the players, Alice, can ascertain whether the total number of distributed apples is even or odd. The only communication allowed is that each of the other two players can send 1 bit to Alice after seeing the number of apples each of them got. Assuming that each of the 32 possible variations of apples occurs with the same probability and using only classical communication, Alice cannot guess the correct answer in more than 75% of the cases. However, the players can always win if each has a qubit of a trio prepared in the state $|\mathrm{GHZ}\rangle$ given in Eq. (1), and each player $j$ applies to his qubit the rotation

$$R(n_j)=|y_0\rangle\langle y_0|+e^{in_j\pi}|y_1\rangle\langle y_1|, \tag{37}$$

where $n_j$ is his number of apples, and then measures the spin of his qubit along the $z$ direction. Finally, Bob and Charlie send their outcomes to Alice. The success of the method is guaranteed by the following property:

$$R(n_A)\otimes R(n_B)\otimes R(n_C)|\mathrm{GHZ}\rangle \\ =\begin{cases}|\mathrm{GHZ}\rangle & \text{if } n_A+n_B+n_C \text{ is even}\\ |\mathrm{GHZ}^{\perp}\rangle & \text{if } n_A+n_B+n_C \text{ is odd,}\end{cases} \tag{38}$$

where

$$|\mathrm{GHZ}^{\perp}\rangle=\frac{i}{2}(|z_0,z_0,z_1\rangle+|z_0,z_1,z_0\rangle+|z_1,z_0,z_0\rangle \\ -|z_1,z_1,z_1\rangle), \tag{39}$$

can be reliably distinguished from $|\mathrm{GHZ}\rangle$ by local measurements along the $z$ direction. This method assumes that all players *share a reference frame* during the protocol. However, such an assumption is not needed if each player replaces his qubit belonging to a trio prepared in $|\mathrm{GHZ}\rangle$ by four qubits belonging to a dozen prepared in $|\Psi\rangle$. The local operations [i.e., the rotation $R(n_j)$ and the measurement along the $z$ direction] are replaced by a protocol, using only single-qubit measurements, for reliably distinguishing between two four-particle states which are invariant under $U_j\otimes U_j\otimes U_j\otimes U_j$.

### C. Quantum cryptography

Other application in which the use of GHZ states provides advantages over any classical protocol is the secret sharing scenario [34–37]: Alice wishes to convey a cryptographic key to Bob and Charlie in such a way that they both can read it only if they cooperate. In addition, they wish to prevent any eavesdropper from acquiring any information without being detected. It is assumed that the players share no previous secret information nor any secure classical channel but, although it is not usually explicitly stated, it is assumed that all three parties *share a reference frame*. Once more, such a requirement can be removed if we replace the GHZ state with the state $|\Psi\rangle$, and the measurements of $Z$ and $X$ with measurements of $\mathcal{Z}$ and $\mathcal{X}$.

### D. Conclusion

To sum up, the interest in rotationally invariant states (i.e., those invariant under $U\otimes\cdots\otimes U$, where $U$ is a unitary operation) goes beyond their use for decoherence-free fault-tolerant universal quantum computation [10–13], solving the Byzantine agreement problem [38–40], and transmitting classical and quantum information between parties who do not share a reference frame [13,41]. *Entangled* rotationally invariant states (i.e., those invariant under $U_A\otimes\cdots\otimes U_A\otimes\cdots\otimes U_N\otimes\cdots\otimes U_N$), like the state $|\Psi\rangle$ given in Eq. (8), can be used to overcome certain assumptions in the proofs of nonexistence of hidden variables, can be applied to reduce the communication complexity of certain tasks, even if the parties do not share any reference frame, and to distribute secret keys among parties who do not share unspeakable information.

### ACKNOWLEDGMENTS

This paper was sparked by a question raised by H. Weinfurter about the possibility of developing a GHZ-like proof of Bell's theorem involving observers who do not share a reference frame and using only single-qubit measurements. I would like to thank him and M. Bourennane for useful discussions on this and related subjects, N. D. Mermin and A. Peres for their comments on a preliminary version, and I. García-Pelayo for sending me the proofs of Ref. [1]. This work was supported by the Spanish Ministerio de Ciencia y Tecnología Project No. BFM2002-02815 and the Junta de Andalucía Project No. FQM-239.

[1] I. García-Pelayo and G. García-Pelayo, *La Fabulosa Historia de Los Pelayos* (Plaza & Janés, Barcelona, 2003).

[2] L. Vaidman, Found. Phys. **29**, 615 (1999).

[3] N.D. Mermin, Phys. Today **43**(6), 9 (1990); reprinted in *Quantum Computation and Quantum Information Theory: Collected Papers and Notes*, edited by C. Macchiavello, G.M. Palma, and A. Zeilinger (World Scientific, Singapore, 2000), p. 53.

[4] N.D. Mermin, Am. J. Phys. **58**, 731 (1990).

[5] D.M. Greenberger, M.A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, Holland, 1989), p. 69; reprinted in *Quantum Computation and Quantum Information Theory: Collected Papers and Notes* (Ref. [3]), p. 49.

[6] D.M. Greenberger, M.A. Horne, and A. Zeilinger, in *Sixty-two Years of Uncertainty: Historical, Philosophical and Physical Inquiries into the Foundations of Quantum Mechanics*, edited by A.I. Miller (Plenum, New York, 1990).

[7] D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[8] A. Peres and P.F. Scudo, in *Quantum Theory: Reconsideration of Foundations*, edited by A. Khrennikov (Växjö University Press, Växjö, Sweden, 2002).

[9] G. Svetlichny, Phys. Rev. D **35**, 3066 (1987).

[10] J. Kempe, D. Bacon, D.A. Lidar, and K.B. Whaley, Phys. Rev. A **63**, 042307 (2001).

[11] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[12] D.A. Lidar, I.L. Chuang, and K.B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[13] M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, and H. Weinfurter, e-print quant-ph/0309041.

[14] This shows the limited scope of the assertion: "there does not exist a rotationally invariant GHZ state of three or more particles" [A. Cabello, Phys. Rev. A **67**, 032107 (2003)].

[15] J. Walgate, A.J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).

[16] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[17] N.D. Mermin (private communication).

[18] A. Cabello, e-print quant-ph/0303076.

[19] S. Kochen and E.P. Specker, J. Math. Mech. **17**, 59 (1967).

[20] N.D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).

[21] N.D. Mermin, Rev. Mod. Phys. **65**, 803 (1993).

[22] D.A. Meyer, Phys. Rev. Lett. **83**, 3751 (1999).

[23] A. Kent, Phys. Rev. Lett. **83**, 3755 (1999).

[24] R. Clifton and A. Kent, Proc. R. Soc. London, Ser. A **456**, 2101 (2000).

[25] H. Havlicek, G. Krenn, J. Summhammer, and K. Svozil, J. Phys. A **34**, 3071 (2001).

[26] N.D. Mermin, e-print quant-ph/9912081.

[27] D.M. Appleby, Phys. Rev. A **65**, 022105 (2002).

[28] A. Cabello, Phys. Rev. A **65**, 052101 (2002).

[29] J.-Å. Larsson, Europhys. Lett. **58**, 799 (2002).

[30] T. Breuer, Phys. Rev. Lett. **88**, 240402 (2002).

[31] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[32] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, Phys. Rev. A **60**, 2737 (1999).

[33] A.M. Steane and W. van Dam, Phys. Today **53**(2), 35 (2000).

[34] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[35] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[36] W. Tittel, H. Zbinden, and N. Gisin, e-print quant-ph/9912035.

[37] A. Cabello, e-print quant-ph/0009025.

[38] M. Fitzi, N. Gisin, and U. Maurer, Phys. Rev. Lett. **87**, 217901 (2001).

[39] A. Cabello, Phys. Rev. Lett. **89**, 100402 (2002).

[40] A. Cabello, Phys. Rev. A **68**, 012304 (2003).

[41] S.D. Bartlett, T. Rudolph, and R.W. Spekkens, Phys. Rev. Lett. **91**, 027901 (2003).