Multipartite nonlocality without entanglement in many dimensions

J. Niset and N. J. Cerf
Quantum Information and Communication, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium
(Received 28 June 2006; published 3 November 2006)

We present a generic method to construct a product basis exhibiting nonlocality without entanglement with n parties each holding a system of dimension at least $n-1$. This basis is generated via a quantum circuit made of controlled discrete Fourier transform gates acting on the computational basis. The simplicity of our quantum circuit allows for an intuitive understanding of this new type of nonlocality. We also show how this circuit can be used to construct unextendible product bases and their associated bound entangled states. To our knowledge, this is the first method which, given a general Hilbert space $\mathcal{H}=\otimes_{i=1}^{n}\mathcal{H}_{d_i}$ with $d_i \leqslant n-1$, makes it possible to construct (i) a basis exhibiting nonlocality without entanglement, (ii) an unextendible product basis, and (iii) a bound entangled state.

DOI: 10.1103/PhysRevA.74.052103 PACS number(s): 03.65.Ud, 03.67.Mn, 03.67.−a

I. INTRODUCTION

One of the most intriguing feature of quantum mechanics is entanglement. As shown in the early 20th century by Einstein, Podolsky, and Rosen, quantum entanglement can give rise to nonlocality, namely the fact that spatially separated systems may behave in a way that cannot be explained by any local theory [1]. This effect, although it does not violate causality, may nevertheless be verified experimentally, as originally discovered by Bell [2]. More specifically, one can write a Bell inequality that must be obeyed by any local realistic model but is violated by quantum mechanics.

Interestingly, there also exist other types of nonlocal behaviors, which go beyond entanglement. Inspired by an early work of Peres and Wootters on a nonlocal effect manifested by correlated product states [3], Bennett *et al.* discovered a set of nine orthogonal product states in $3\otimes 3$ dimensions that cannot be perfectly distinguished if the two parties are restricted to local operations and classical communications (LOCC) [4]. This behavior was termed "nonlocality without entanglement" (NLWE) since we have a truly nonlocal behavior while entanglement is used neither in the preparation of the states, nor in the joint measurement that discriminates them perfectly. In contrast, the model of Peres and Wootters concerned the joint measurement of a pair of qubits prepared in a product (hence nonentangled) state via an observable admitting entangled eigenstates; they exhibited an example with correlated qubits where such a measurement gives more information than a separate LOCC-type measurement.

The NLWE behavior can be viewed as a new striking example of the nonequivalence between the concept of quantum entanglement and that of quantum nonlocality. It was know since Werner [5] that entanglement does not necessarily imply nonlocality in the sense of producing data that are incompatible with local realism (entanglement$\neRightarrow$nonlocality). This new type of nonlocality implies that the converse does not hold either (nonlocality$\neRightarrow$entanglement). Note that nonlocality is not understood here as the incompatibility with local realism, but instead as the advantage of a joint measurement with respect to all LOCC strategies. More generally, NLWE thus raises the question: what kind of global operations can or cannot be performed using LOCC operations only? This question has attracted a lot of attention over the recent years as it underpins the use of entanglement as a resource in quantum information theory.

Walgate *et al.* [6] have shown that any two orthogonal quantum states, entangled or not, can be reliably distinguished using LOCC. Later, Walgate and Hardy [7] established the necessary and sufficient conditions for a general set of 2×2 quantum states to be locally distinguishable, and for a general set of $2\times n$ to be distinguished given an initial measurement of the qubit. These results reveal a fundamental *asymmetry* inherent to local distinguishability, which is conjectured to be at the origin of NLWE. For example, there exist sets of bipartite orthogonal product states that cannot be reliably distinguished locally if Bob is to go first and only one-way communication from him to Alice is allowed, but can be distinguished if Alice performs the first sequence of measurements and then shares her results with Bob. One such set is given by

$$\begin{aligned} |\Psi_1\rangle &= |0\rangle_a|0\rangle_b, \\ |\Psi_2\rangle &= |0\rangle_a|1\rangle_b, \\ |\Psi_3\rangle &= |1\rangle_a|0+1\rangle_b, \\ |\Psi_4\rangle &= |1\rangle_a|0-1\rangle_b, \end{aligned} \tag{1}$$

where $\{|0\rangle, |1\rangle\}$ stands for the computational basis (CB) while $\{|0\pm 1\rangle\}=\{\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)\}$ stands for the dual basis (DB). Groisman and Vaidman [8] studied the "one-way indistinguishability" exhibited by this simple set, and used it to construct an alternative proof of the NLWE of the nine states found by Bennett *et al.* [4].

In this paper, we further investigate this close connection between NLWE and one-way indistinguishability by introducing a two-qubit quantum gate called the controlled-HADAMARD (controlled-H). This gate applies a Hadamard transform to one of the qubits conditioned on the other qubit being in the appropriate state of the CB, say $|1\rangle$. Not surprisingly, this gate is closely connected to the set (1) since it generates (1) when applied on the four states of the CB. This

controlled-HADAMARD gate can be easily generalized to the n-partite case with d-dimensional systems: the Hadamard transform becomes a d-dimensional quantum discrete Fourier transform (DFT) applied to the nth system, while the control extends to the $n-1$ first parties. We will refer to this gate as a controlled-DFT_d in the following.

In Sec. II, we will show that this controlled-H gate provides us with a nice formalism to understand the mechanism of NLWE. Based on our observations of a known set exhibiting this phenomena, namely, the so-called SHIFT ensemble introduced in Ref. [4], we will derive in Sec. III a generic method to construct multipartite product bases exhibiting NLWE with systems of arbitrary dimension. Finally, in Secs. IV and V, we will exploit the fact that NLWE is connected to other peculiar quantum phenomena such as unextendible product bases (UPB) [9,10] and bound entanglement (BE) [11,12], and will apply our method to generalize the construction of a large variety of UPBs and related BE states, a task that has proven to be extremely difficult in the past.

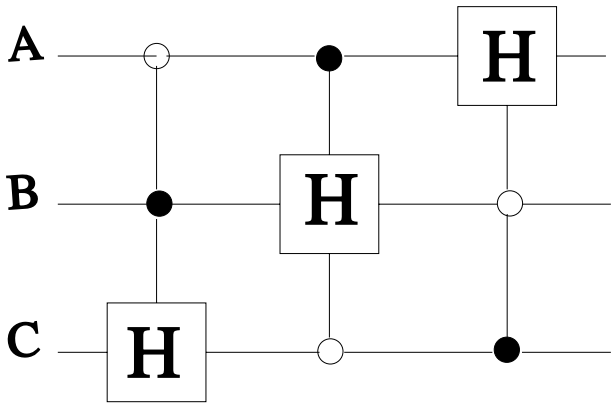

FIG. 1. Quantum circuit generating the SHIFT ensemble from the computational basis. The empty and filled circles correspond to a control condition of $|0\rangle$ and $|1\rangle$, respectively. For example, the first gate applies a Hadamard to Charles' qubit if Alice's qubit is $|0\rangle$ and Bob's qubit is $|1\rangle$.

II. NONLOCALITY WITHOUT ENTANGLEMENT

The SHIFT ensemble defined in [4] is the following set of eight orthogonal three-qubit product states

$$
\begin{aligned}
|\Psi_1\rangle &= |0\rangle_a|0\rangle_b|0\rangle_c,\\
|\Psi_2\rangle &= |0+1\rangle_a|0\rangle_b|1\rangle_c,\\
|\Psi_3\rangle &= |0\rangle_a|1\rangle_b|0+1\rangle_c,\\
|\Psi_4\rangle &= |0\rangle_a|1\rangle_b|0-1\rangle_c,\\
|\Psi_5\rangle &= |1\rangle_a|0+1\rangle_b|0\rangle_c,\\
|\Psi_6\rangle &= |0-1\rangle_a|0\rangle_b|1\rangle_c,\\
|\Psi_7\rangle &= |1\rangle_a|0-1\rangle_b|0\rangle_c,\\
|\Psi_8\rangle &= |1\rangle_a|1\rangle_b|1\rangle_c. \qquad (2)
\end{aligned}
$$

To understand why this set exhibits NLWE, consider the following game. An external party randomly chooses a number between 1 and 8 and accordingly prepares the corresponding quantum state $|\Psi_i\rangle$. He then sends the shares of this state to Alice, Bob, and Charles, who are located, respectively, at A, B, and C, and asks them to identify the state they have received, i.e., to perfectly determine the value of i. Note that Alice, Bob, and Charles know the precise form of the states of the set, but ignore which one has been prepared. To distinguish between the possible states, the players may have recourse to LOCC only. This means that they are allowed to perform any sequence of local operations or measurements on their respective shares of the state and communicate their results to the other players through a classical channel, but cannot perform a joint measurement or communicate through a quantum channel. Indeed, if the players had access to joint operations, the problem would be trivial since the states are orthogonal, hence perfectly distinguishable. Surprisingly, it turns out that when the set of operations is restricted to LOCC, the players will never be able to perfectly distinguish between the eight possible states [4]. Although the set is made of orthogonal product states, which can thus be prepared locally, it has the property of being locally indistinguishable (throughout this paper, we use indistinguishable to mean not perfectly distinguishable).

It is interesting to investigate how the joint measurement, which perfectly discriminates between the states of the set, can be implemented in terms of quantum logic gates. Formally, it is a projective measurement based on the eight projectors onto product states $\Pi_i=|\Psi_i\rangle\langle\Psi_i|$. Consider the three-qubit unitary operation U, which transforms the eight states of the CB onto the states of the SHIFT ensemble $|\Psi_i\rangle$. The knowledge of this joint unitary operation U gives a simple strategy to perform the joint measurement: it can be decomposed as the sequence of the joint unitary operation $U^\dagger$ followed by a local measurement by Alice, Bob, and Charles in the computational basis. Interestingly, it turns out that the unitary U can be implemented by a simple quantum circuit made of three identical controlled-HADAMARD gates. As seen in Fig. 1, this gate is a tripartite gate which applies a Hadamard transform onto one of the qubits conditioned on the other two being in the appropriate product state $|0\rangle$ $|1\rangle$. More precisely, in case the Hadamard acts on Charles' qubit, this controlled-H gate performs the operation

$$
|i\rangle_a|j\rangle_b|k\rangle_c \rightarrow \begin{cases} |i\rangle_a|j\rangle_b H|k\rangle_c & \text{if } i=0 \wedge j=1,\\ |i\rangle_a|j\rangle_b|k\rangle_c & \text{otherwise,}\end{cases}
$$

with $H|0\rangle=|0+1\rangle$ and $H|1\rangle=|0-1\rangle$. Because of the cyclic control conditions, the three gates appearing in the circuit for U are commuting; one can easily check that if the control conditions are satisfied for one of the gates, they cannot be satisfied for the two others. We will call this property "exclusivity." As an example, consider the first and second gates of the circuit. Expressing the Hadamard as $H=\exp(iG)$ with

$G=(\pi/2)(\mathbb{1}-H)$, these two gates can be written, respectively, as $\exp(iA)$ and $\exp(iB)$ with

$$A = \frac{1}{4}(\mathbb{1} + \sigma_z) \otimes (\mathbb{1} - \sigma_z) \otimes G,$$

$$B = \frac{1}{4}(\mathbb{1} - \sigma_z) \otimes G \otimes (\mathbb{1} + \sigma_z).$$

We deduce from these expressions that $AB=BA=0$ since it contains the product $(\mathbb{1}+\sigma_z)(\mathbb{1}-\sigma_z)=0$, which translates the exclusivity property. Hence, $[A,B]=0$, and the Baker-Campbell-Hausdorff formula gives

$$e^{iA}e^{iB} = e^{i(A+B)}e^{-[A,B]/2} = e^{i(A+B)}e^{[A,B]/2} = e^{iB}e^{iA}$$

which proves the commutation between the first and second gates of the circuit (the same reasoning holds for any two gates).

Why does the circuit works? Consider first the ensemble constructed by applying only the first controlled-H (the one that acts on Charles' qubit) on the states of the CB. As shown in Refs. [7,8], this ensemble is indistinguishable if Charles is forced to perform the first nontrivial step of the measurement strategy, or equivalently if he is restricted to one-way classical communication towards Alice and Bob. This is obvious as his share of the state could either be in the computational or in the dual basis, and any nontrivial measurement (one that will gain some information about one of these bases) will always irreversibly lose some information about the conjugate basis. Of course, if Alice and Bob start while Charles is allowed to delay his measurement, then the set appears perfectly distinguishable. Alice and Bob should simply measure in the CB and then inform Charles about the basis he should use. This is what Walgate and Hardy called the "asymmetry of local distinguishability."

Next, let us play the same game but using a quantum circuit made of the two first controlled-H gates (those acting on Charles' and Bob's qubits). The fact that the two gates are commuting (and exclusive) guarantees that no entanglement will be created when the sates of the CB are processed, i.e., the product states of the CB transform into another set of product states. This time, the ensemble appears indistinguishable to both Charles and Bob as their shares of the states are made of.nonorthogonal, hence indistinguishable, states. This is obvious if we adopt a measurement point of view. The second gate tells us that Bob cannot start. But, since the gates commute, the second gate can be interchanged with the first, leading to the similar conclusion that Charles cannot start. Thus, in order to perfectly distinguish the states locally, neither Bob nor Charles may start. Again, if it is Alice who goes first, then the ensemble becomes locally distinguishable. She simply measures her share of the state in the CB: if she gets a $|0\rangle$ she knows that Bob's share should be measured in the CB, and the outcome of Bob's measurement determines which basis Charles should use. A $|1\rangle$ simply interchanges Charles' and Bob's roles. In short, this ensemble is locally indistinguishable if Charles or Bob are forced to start, but distinguishable if Alice goes first.

Now, consider the entire circuit of Fig. 1, that is, the circuit made of the three controlled-H gates and the SHIFT ensemble that it generates. Following the two previous examples, we know that this ensemble is locally indistinguishable as each player sees an indistinguishable subset created by the Hadamard gate acting on his qubit (this gate can be placed last in the circuit). Consequently, in this case *nobody* wants to start. Because in every LOCC strategy, *someone* has to start, we get a simple picture of why the SHIFT ensemble exhibits NLWE. This can be summarized as follows: (1) in every LOCC strategy, someone has to start; (2) the last gate implies that Alice cannot start; (3) the gates commute and can thus be interchanged; (4) as a consequence of statements (2) and (3), nobody wants to start; (5) statements (1) and (4) are incompatible.

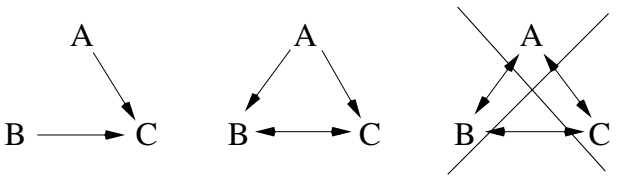

FIG. 2. In the first game (left), Charles needs information from both Alice and Bob to make the set distinguishable. In the second game (middle), Bob needs to receive information from Alice and transmit information to Charles, or the reverse, depending on Alice's measurement. In the third scenario (right), even if the players have access to all possible classical communication protocols, the set remains locally indistinguishable (NLWE).

The three scenarios we have presented and the corresponding LOCC strategies can be nicely illustrated with the diagrams of Fig. 2. The arrows represent the minimum amount of communication required to make the ensemble locally distinguishable. This intuitive picture will be translated into a rigorous proof in the next section.

III. *N*-PARTITE NONLOCALITY WITHOUT ENTANGLEMENT IN ARBITRARY DIMENSION

With the intuition gained from our circuit, we see that what is really at issue in NLWE is not the kind of LOCC protocols employed by the parties, nor the content of their communication, but rather the asymmetry of local distinguishability encapsulated in the states themselves. Indeed, it is because each player does not know which of the two conjugated basis he should use to measure his share of the state (the set is indistinguishable from his point of view) and because all players are in this same situation (the gates commute) that the ensemble is locally indistinguishable as a whole. All we have used so far is thus the possibility, for each player, to have a state belonging to two conjugate bases. We may therefore extend our construction to systems of arbitrary dimension instead of qubits. Given the central role played by the controlled-H gate, which creates this local indistinguishability, we may replace it with a d-dimensional quantum discrete Fourier transform (DFT_d). This yields a simple strategy to construct an ensemble made of orthogonal tripartite product states of arbitrary dimensions that exhibits NLWE. Note that by changing the control conditions of the

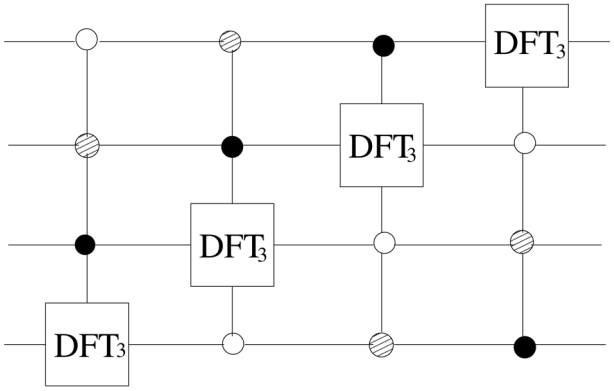

FIG. 3. Nonlocality without entanglement in dimension $3\otimes 3\otimes 3\otimes 3$. The first gate applies a discrete Fourier transform in dimension 3 to Damian's qutrit if Alice's state is a $|0\rangle$, Bob's state a $|1\rangle$, and Charles' state a $|2\rangle$.

gates while maintaining their exclusivity, we can define a whole family of NLWE ensembles with equivalent properties. Furthermore, there is no need to restrict the circuit to a tripartite scenario. Knowing that the key ingredient is a sequence of controlled-DFT gates that are exclusive (hence commuting), we can further generalize the method and increase the number of parties. The quantum circuit will now be made of n controlled-DFT gates, one acting on each player, and we require these gates to be exclusive to make sure that the resulting ensemble is made of product states. This imposes some constraint on the dimensions of the players' shares. A simple way to satisfy this exclusivity condition is to require that each player has a Hilbert space large enough to accommodate $n-1$ gates with a different control state. We can therefore state the following sufficient condition:

$$d_j \geqslant n-1, \tag{3}$$

where d_j is the dimension of $\mathcal{H}_j$, the Hilbert space of player j, and n is the total number of players. We thus have established a generic method to construct some n-partite ensemble of product states exhibiting NLWE using systems of arbitrary dimension:

Statement. If we have $n\geqslant 3$ parties working in respective Hilbert spaces $\mathcal{H}_j$ of dimension $d_j\geqslant n-1$, a quantum circuit can be defined, based on n controlled-DFT gates, which generates a set $\{|\Psi_i\rangle\}$ made of $\Pi_j d_j$ orthogonal product states that form a basis of $\mathcal{H}=\otimes_j\mathcal{H}_j$ and exhibit nonlocality without entanglement.

Proof. Let us denote the CB of player j by $\{|0\rangle,\cdots|d_j-1\rangle\}$. We consider the ensemble generated from the CB of all players by applying the unitary

$$U=\prod_{j=1}^{n} e^{iA_j} \tag{4}$$

with $A_1=\otimes_{j=1}^{n-1}|j-1\rangle\langle j-1|\otimes G$ and $A_{2,3,\ldots,n}$ are cyclic permutations of A_1. In the simplest case, each party has a dimension $d_j=n-1$, saturating relation (3), but this is not necessary for the proof to hold. As an example, we show in Fig. 3 the circuit generating this simplest ensemble exhibiting NLWE for a quadripartite scenario in which all parties hold a qutrit, i.e., in a Hilbert space of total dimension $3\otimes 3\otimes 3\otimes 3$.

Let us proof now that the ensemble generated by Eq. (4) exhibits NLWE. Suppose Alice has a share of dimension d and performs the first step of the measurement procedure. We will show that, under the simple constraint of not allowing her operation to lead to a situation in which it has become impossible in principle to perfectly distinguish between the initial states $|\Psi_i\rangle$, then she cannot gain any information. First, let us rewrite the states of the ensemble as $|\Psi_i\rangle=|\phi_i\rangle_A|\varphi_i\rangle_B$, where $|\phi_i\rangle$ is Alice's share and $|\varphi_i\rangle_B$ is the state held by all the other players. We describe Alice's measurement in two stages: first, her share of the state and the measuring device evolve unitarily under the action of some unitary operator U_A; second, some outcome k is read out. The unitary evolution of Alice's share and the measuring device can be described by

$$U_A:|\phi_i\rangle_A|A\rangle\rightarrow\sum_k \alpha_{ik}|\omega_{ik}\rangle, \tag{5}$$

where $|A\rangle$ is the initial state of the measuring device and $|\omega_{ik}\rangle$ is the joint state of Alice's share and the measuring device corresponding to a particular outcome k. Without restriction, we can choose α_{ik} to be real and non-negative. Importantly, the states $|\omega_{i,k}\rangle$ with different k must be orthogonal as they correspond to different outcomes of the macroscopic measuring device. Note that Alice only sees $2d$ distinct states $|\phi_i\rangle_A$, the d states of the CB and the d states of the DB. Thus, for each k, it is sufficient to introduce $2d$ couples $\{\alpha_{ik},|\omega_{ik}\rangle\}$, and we can write the action of the unitary operation U_A on these $2d$ different states $|\phi_i\rangle_A$ as

$$|m\rangle_A\otimes|A\rangle\xrightarrow{U_A}\sum_k \alpha_{m,k}|\omega_{m,k}\rangle,$$

$$\|m\rangle_A\otimes|A\rangle\xrightarrow{U_A}\sum_k \alpha'_{m,k}|\omega'_{m,k}\rangle \tag{6}$$

with k labeling the different outcomes, $m=0,\ldots,d-1$, and $\|m\rangle$ denoting the states of the DB.

Next, we must impose some constraints on Alice's possible operations. On the one hand, she has to distinguish between the d states that are in the DB at her side since these states appear identical to the other parties. On the other hand, there are also states that are in the CB but are only distinguishable by Alice as they appear nonorthogonal to the other parties [e.g., the states $|\Psi_3\rangle$ and $|\Psi_8\rangle$ of the ensemble (2), or the states $|0\rangle_A|2\rangle_B|2\rangle_C|2\rangle_D$ and $|1\rangle_A|2\rangle_B|2\rangle_C|2\rangle_D$ in the example of Fig. 3]. For those states, which she sees as orthogonal, she must maintain perfect distinguishability whatever action she performs and for every value of the outcome k. In other words, her measurement must either distinguish these states outright or leave them orthogonal, i.e., we must impose for every k and for all $m\neq n=0,1,\ldots,d-1$

$$\alpha_{m,k}\alpha_{n,k}\langle\omega_{m,k}|\omega_{n,k}\rangle=0,$$

$$\alpha'_{m,k}\alpha'_{n,k}\langle\omega'_{m,k}|\omega'_{n,k}\rangle = 0. \tag{7}$$

In addition to these $d(d-1)$ constraints, we also need to consider the relations between the possible initial states at Alice's site. More precisely, we know that the CB and DB are related by the quantum Fourier transform

$$\|n\rangle = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} \exp\left(i\frac{2\pi}{d}nl\right)|l\rangle,$$

$$|m\rangle = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} \exp\left(-i\frac{2\pi}{d}ml\right)\|l\rangle. \tag{8}$$

The unitary evolution U_A must conserve these relations and, since $|\omega_{m,k}\rangle$ with different k are orthogonal, we can write $2d$ relations of the form

$$\alpha'_{lk}|\omega'_{lk}\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} \exp\left(i\frac{2\pi}{d}jl\right)\alpha_{jk}|\omega_{jk}\rangle,$$

$$\alpha_{lk}|\omega_{lk}\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} \exp\left(-i\frac{2\pi}{d}jl\right)\alpha'_{jk}|\omega'_{jk}\rangle \tag{9}$$

for each outcome k, with $l=0,\ldots,d-1$. Consider the last d relations of Eq. (9). If we take the scalar product of two of them and reorganize appropriately the different terms of the sums, we obtain

$$\alpha_{lk}\alpha_{l'k}\langle\omega_{lk}|\omega_{l'k}\rangle = \frac{1}{d}\left[\sum_{j=0}^{d-1} \exp\left(-i\frac{2\pi}{d}j(l-l')\right)\alpha'^2_{jk} + 2\sum_{j=0}^{d-1}\sum_{j'>j} \cos\left(\frac{2\pi}{d}(lj-l'j')\right) \times \alpha'_{jk}\alpha'_{j'k}\langle\omega'_{j'k}|\omega'_{jk}\rangle\right]. \tag{10}$$

If we now choose $l=l'$, it follows that

$$\alpha^2_{lk} = \frac{1}{d}\left[\sum_{j=0}^{d-1}\alpha'^2_{jk} + 2\sum_{j=0}^{d-1}\sum_{j'>j}\cos\left(\frac{2\pi}{d}l(j-j')\right) \times \alpha'_{jk}\alpha'_{j'k}\langle\omega'_{j'k}|\omega'_{jk}\rangle\right] \tag{11}$$

By the second condition of Eq. (7), all the terms of the second sum of the right-hand side are trivially equal to zero. Since the remaining term does not depend on the value of l, we conclude that, for each value of the outcome k, all the α_{lk}'s are equal. Similarly, from the other d conjugated relations of Eq. (9), we conclude that for all k the α'_{lk}'s must be equal and equal to the α_{lk}'s. It follows that if k is a possible outcome for one particular initial state $|\psi_i\rangle$, then k is a possible outcome for all the initial states. In addition, for all such outcomes k the distinguishability condition (7) becomes the true orthogonality condition

$$\langle\omega_{mk}|\omega_{nk}\rangle = 0 \quad \forall\, m \neq n \in \{0,1,\cdots d-1\},$$

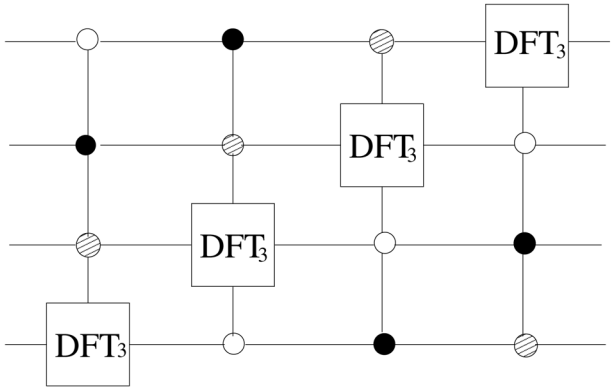

FIG. 4. By concatenating this circuit to the one of Fig. 3, one gets another ensemble exhibiting NLWE in dimension $3\otimes 3\otimes 3\otimes 3$. The first gate applies a discrete Fourier transform in dimension 3 to Damian's qutrit if Alice's state is a $|0\rangle$, Bob's state a $|2\rangle$, and Charles' state $|1\rangle$.

$$\langle\omega'_{mk}|\omega'_{nk}\rangle = 0 \quad \forall\, m \neq n \in \{0,1,\cdots d-1\}. \tag{12}$$

To summarize, after a measurement procedure which produced the outcome k, the set of possible initial states of Alice's share together with the measuring device have evolved into a set of states which is isomorphic to the initial set, i.e., no information can be gained and communicated to the other players from the value of k. Thus, in order to perfectly distinguish between the states, Alice cannot start. In view of the commutation of the gates, similar arguments can be used to show that the other players face the same dilemma of either gaining some useful information at the cost of irreversibly losing perfect distinguishability, or not gaining any information at all. This completes the proof. ■

To conclude this section, it is worth noticing that the sets we have constructed so far are not the most general ones. Indeed, for $d>2$ the size of the local Hilbert space allows for the introduction of more gates without loosing the exclusivity (or commutation) condition. For instance, a gate triggered by $|0\rangle_A|2\rangle_B|1\rangle_C$ and acting on Damian's qutrit can be added to the circuit of Fig. 3 while conserving the commutation condition. The set constructed with the circuit of Fig. 3 supplemented with this gate and cyclic permutations (as shown in Fig. 4) exhibits NLWE while it is qualitatively distinct from the set of Fig. 3. In particular, it has more shares in the dual bases, so we conjecture that it should be "more nonlocal" in this respect. Nevertheless, for the rest of this paper we will only consider sets constructed with the minimum number of gates n. As a last comment, let us note that although our method *as it is* fails to create bipartite NLWE, the nine bipartite qutrit states ("domino" states) of Ref. [4] do fit into our picture of commuting control gates. We can associate to this set a quantum circuit made of four control gates, two for each player, where the exclusivity of the gates requires the Fourier transform to act on two-dimensional subspaces of $\mathcal{H}_A$ and $\mathcal{H}_B$.

IV. *N*-PARTITE UNEXTENDIBLE PRODUCT BASES

Definition. Consider a n-partite quantum system belonging to $\mathcal{H}=\otimes_{i=1}^{n}\mathcal{H}_i$, with the local Hilbert spaces of respective

dimensions d_i. An unextendible product basis is an incomplete orthogonal product basis whose complementary subspace contains no product state.

Unextendible product bases (UPBs) are known to be closely connected to NLWE. More precisely, Bennett *et al.* [9] showed that the members of a UPB cannot be perfectly distinguished if one is restricted to LOCC, i.e., they exhibit NLWE (see also Ref. [13]). A necessary and sufficient condition for extendibility of a product basis is also known, and has been used to construct a UPB from a complete product basis exhibiting NLWE. This method was used, for example, to construct the following UPB:

$$|\Psi_4\rangle = |0\rangle_a|1\rangle_b|0-1\rangle_c,$$

$$|\Psi_6\rangle = |0-1\rangle_a|0\rangle_b|1\rangle_c,$$

$$|\Psi_7\rangle = |1\rangle_a|0-1\rangle_b|0\rangle_c,$$

$$|\Psi_{\mathrm{st}}\rangle = |0+1\rangle_a|0+1\rangle_b|0+1\rangle_c \tag{13}$$

from the SHIFT ensemble [9,10]. The extra state $|\Psi_{\mathrm{st}}\rangle$ here stands for the "stopper" state, as explained later on. Since we have found in the previous section a systematic way of creating product bases exhibiting NLWE, we can further exploit these ideas and give a systematic protocol to construct UPBs based on quantum circuits such as those of Fig. 1 and 3. Although the protocol we present here most probably does not account for the construction of all possible UPBs, it nevertheless can be used to construct a family of UPBs in a large variety of scenarios.

We will illustrate the construction with a simple example. Consider the quadripartite circuit of Fig. 3 and suppose Alice, Bob, Charles, and Damian hold systems of dimension d_a, d_b, d_c, and d_d, respectively. We have shown that this circuit generates an ensemble $\{|\Psi_i\rangle\}$ made of $d_a d_b d_c d_d$ orthogonal product states exhibiting NLWE. We construct an UPB out of $\{|\Psi_i\rangle\}$ by extracting from it the d_a-1 states in which Alice's share is any state of the DB except the last one, the d_b-1 states in which Bob's share is any state of the DB except the last one, the d_c-1 states in which Charles' share is any state of the DB except the last one, and the d_d-1 states in which Damian's share is any state of the DB except the last one. We complete these $\Sigma_{i=1}^4(d_i-1)$ states by adding a proper *stopper* state, so as to force the unextendibility of the set. Note that the number of states m in a UPB is known to verify the condition [9]

$$m \geqslant \sum_{i=1}^{n} (d_i - 1) + 1 \tag{14}$$

so that the above construction yields a minimal UPB.

More specifically, the UPB consists of the states

$$|\Psi_1^0\rangle = |0\rangle_a|1\rangle_b|2\rangle_c F|0\rangle_d,$$

$$\vdots$$

$$|\Psi_1^{d_d-2}\rangle = |0\rangle_a|1\rangle_b|2\rangle_c F|d_d-2\rangle_d,$$

$$|\Psi_2^0\rangle = |1\rangle_a|2\rangle_b F|0\rangle_c|0\rangle_d,$$

$$\vdots$$

$$|\Psi_2^{d_c-2}\rangle = |1\rangle_a|2\rangle_b F|d_c-2\rangle_c|0\rangle_d,$$

$$|\Psi_3^0\rangle = |2\rangle_a F|0\rangle_b|0\rangle_c|1\rangle_d,$$

$$\vdots$$

$$|\Psi_3^{d_b-2}\rangle = |2\rangle_a F|d_b-2\rangle_b|0\rangle_c|1\rangle_d,$$

$$|\Psi_4^0\rangle = F|0\rangle_a|0\rangle_b|1\rangle_c|2\rangle_d,$$

$$\vdots$$

$$|\Psi_4^{d_a-2}\rangle = F|d_a-2\rangle_a\,|0\rangle_b|1\rangle_c|2\rangle_d,$$

$$|\Psi_{\mathrm{st}}\rangle = F|d_a-1\rangle_a F|d_b-1\rangle_b F|d_c-1\rangle F|d_d-1\rangle, \tag{15}$$

where $F|i\rangle$ is the discrete Fourier transform of $|i\rangle$. To understand why this set is unextendible, suppose we want to add a new product state that is orthogonal to it. Clearly, because of the d_a-1 states that are in the DB for Alice together with the stopper sate, we cannot find a state orthogonal to Alice's share (this subset of d_a states span her entire subspace). So, we should try to look for a product state that is orthogonal to this set within Bob's, Charles', or Damian's subspaces. But the same argument as for Alice's subspace can be applied as well. Hence no product state can be found that is orthogonal to all the states, and the set is unextendible.

V. *N*-PARTITE BOUND ENTANGLED STATES

In addition to being locally indistinguishable, UPBs are also connected to another important quantum property, namely, bound entanglement. A bound entangled (BE) state is an entangled mixed state from which no pure entanglement can be distilled [11,12]. The role of bound entanglement in nature, and its yet-to-find possible use for quantum information processing has attracted a lot of attention. Although the construction of bound entangled states has proven to be a difficult task, it has been realized that the state corresponding to the uniform mixture on the subspace orthogonal to a UPB $\{|\tilde{\psi}_i\rangle, i=1,\ldots,m\}$, namely,

$$\hat{\rho} = \frac{1}{D-m}\left(1 - \sum_{i=1}^{m} |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\right) \tag{16}$$

is a bound entangled state [9], where D is the total dimension of the Hilbert space. This is one of the only known generic method to construct bound entangled states. The quantum circuit we have introduced provides us with a simple strategy to construct a large number of UPBs, hence it also provides us with a simple method to construct a large number of BE states. Consider again our quadripartite UPB, as defined in

Eq. (15). By definition the space complementary to the UPB contains no product states, hence $\hat{\rho}$ is entangled. We can use the partial transposition to show that every partitioning of the parties is PPT: indeed, the identity is invariant under partial transposition and the product states $|\tilde{\psi}_i\rangle$ of the UPB are mapped onto other product states. Thus, no entanglement can be distilled across any bipartite cut. In addition, note that if some pure global entanglement could nevertheless be distilled, it could be used to create entanglement across a bipartite cut; hence no entanglement at all can be distilled and the state is indeed bound entangled.

In the special case where the exclusivity condition (3) is saturated, that is, when we have $n=d+1$ parties holding each a system of dimension d, the BE state produced by this method has another interesting property, namely that the entanglement across any $d\otimes d^d$ cut is zero (this is stronger than the nondistillability of bipartite entanglement across any $d\otimes d^d$ cut). This result was already derived for the special case of the SHIFT ensemble [9], i.e., for $d=2$, and we will show here how to use a similar argument to prove that it is the case for any value of d.

To show that the entanglement across the cut $A/BC\cdots E$ is zero, we explicitly separate Alice from the other parties and rewrite the d^2 states of the UPB as

$$|\Psi_{1,i}\rangle = |0\rangle|a_i\rangle, \quad |a_i\rangle = |1,2,\ldots,d-2,F(i)\rangle,$$

$$|\Psi_{2,i}\rangle = |1\rangle|b_i\rangle, \quad |b_i\rangle = |2,\ldots,d-2,F(i),0\rangle,$$

$$\vdots$$

$$|\Psi_{d,i}\rangle = |d-1\rangle|e_i\rangle, \quad |e_i\rangle = |F(i),0,\ldots,d-3\rangle,$$

$$|\Psi_{d+1,i}\rangle = |F(i)\rangle|f\rangle, \quad |f\rangle = |0,\ldots,d-1\rangle,$$

$$|\Psi_{\mathrm{st}}\rangle = |F(d-1)\rangle|g\rangle, \quad |g\rangle = |F(d-1),\ldots,F(d-1)\rangle,$$

where $i=0,\ldots,d-2$, and $F(i)$ means $F|i\rangle$. Next note that $|f\rangle$ and $|g\rangle$ span a Hilbert space $S=\mathrm{span}(f,g)$ of dimension 2, and that all the states in this space are orthogonal to $\{|a_i\rangle,|b_i\rangle,\ldots,|e_i\rangle\}$. We thus define the Hilbert space $S'=\mathcal{H}(d^d)/S$ of dimension d^d-2 such that (i) all the states in this space are, by construction, orthogonal to $|f\rangle$ and $|g\rangle$ and (ii) all the states $\{|a_i\rangle,|b_i\rangle,\ldots,|e_i\rangle\}$ are in S'. We can therefore find an ensemble of d^d-d-1 orthogonal vectors $|a_k^\perp\rangle$ such that every $|a_k^\perp\rangle$ belongs to S' and is orthogonal to all the $|a_i\rangle$, i.e., $\{|a_i\rangle,|a_k^\perp\rangle\}$ is an orthogonal basis of S'. We repeat that procedure for the $\{|b_i\rangle\}$ and define d^d-d-1 vectors $|b_k^\perp\rangle$ in S', until we have defined the last d^d-d-1 vectors $|e_k^\perp\rangle$ associated to the states $\{|e_i\rangle\}$. In addition, we can also define $|f^\perp\rangle$ and $|g^\perp\rangle$ in S, orthogonal to $|f\rangle$ and $|g\rangle$ respectively. We can now use all these new vectors to complete the original UPB and make it a full d^{d+1}-dimensional product basis between A and $BC\cdots E$. This is done by adding the $d(d^d-d-1)+(d-1)+1=d^{d+1}-d^2$ new states $\{|0\rangle|a_k^\perp\rangle,|1\rangle|b_k^\perp\rangle,\ldots,|d-1\rangle|e_k^\perp\rangle,|F(i)\rangle|f^\perp\rangle,|F(d-1)\rangle|g^\perp\rangle\}$. This shows that with respect to the cut A and $BC\cdots E$, the set is completed by product states and the mixed state $\hat{\rho}$ is therefore not entangled. Because the state is symmetric, this argument also applies to the other $d\otimes d^d$ splits which prove that our generic bound entangled state contains no entanglement across any such cuts.

VI. CONCLUSIONS

We have developed a systematic approach to nonlocality without entanglement based on observations of the SHIFT ensemble introduced by Bennett *et al.* [4]. Our approach, centered on commuting controlled-HADAMARD gates, connects NLWE to a simple quantum circuit consisting of such gates. This method gives an intuitive understanding of NLWE, and allows for a generalization both in the number of parties and in the dimension of their spaces. We therefore derive the first method to construct n-partite d-dimensional product bases exhibiting NLWE. For example, in Fig. 3, we display the quantum circuit generating the set exhibiting NLWE with four qutrits; to our knowledge, it is the first example of NLWE in $3\otimes 3\otimes 3\otimes 3$.

The ingredients of our method are very general, and incorporate also the construction of the other known examples of NLWE introduced in Ref. [4]. In contrary to the original work of Ref. [4], we did not attempt to place a bound on the mutual information attainable through LOCC, but rather adopted the strategy of Ref. [8] and restricted ourselves to proving that such a nontrivial bound exists. However, a strategy to calculate this bound is needed as it would allow us to compare the degree of nonlocality exhibited by the different ensembles we can construct with this method, so it is an interesting challenge for future work. Because NLWE is connected to other quantum peculiarities such as unextendible product bases and bound entanglement, our method can be adapted to construct n-partite high-dimensional UPBs and their associated BE states, a task that has proven to be difficult in the past.

ACKNOWLEDGMENTS

We acknowledge financial support from the Communauté Française de Belgique under Grant No. ARC 00/05-251, from the IUAP programme of the Belgian government under Grant No. V-18, and from the EU under projects QAP and SECOQC. J.N. also acknowledges support from the Belgian FRIA foundation.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[3] A. Peres and W. K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).
[4] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[5] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[6] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).
[7] J. Walgate and L. Hardy, Phys. Rev. Lett. **89**, 147901 (2002).
[8] B. Groisman and L. Vaidman, J. Phys. A **34**, 6881 (2001).
[9] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999).
[10] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, Commun. Math. Phys. **238**, 379 (2003).
[11] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[12] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[13] S. De Rinaldis, Phys. Rev. A **70**, 022309 (2004).