Spectral decomposition of Bell's operators for qubits

2001 J. Phys. A: Math. Gen. 34 6043

(http://iopscience.iop.org/0305-4470/34/30/314)

J. Phys. A: Math. Gen. **34** (2001) 6043–6053 PII: S0305-4470(01)23557-4

Spectral decomposition of Bell's operators for qubits

Valerio Scarani[1] **and Nicolas Gisin**

Group of Applied Physics, University of Geneva 20, rue de l'Ecole-de-Médecine, CH-1211 Geneva, Switzerland

E-mail: valerio.scarani@physics.unige.ch

Received 27 March 2001, in final form 19 June 2001
Published 20 July 2001
Online at stacks.iop.org/JPhysA/34/6043

Abstract

The spectral decomposition is given for the N-qubit Bell operators with two observables per qubit. It is found that the eigenstates (when non-degenerate) are N-qubit GHZ states even for those operators that do not allow the maximal violation of the corresponding inequality. We present two applications of this analysis. In particular, we discuss the existence of pure entangled states that do not violate the Mermin–Klyshko inequality for $N \geqslant 3$.

PACS numbers: 03.65.Ud, 03.65.-w

1. Introduction

There is much literature available concerning Bell's inequalities. For the sake of this introduction, we briefly recall some well known ideas, using the Clauser–Horne–Shimony–Holt (CHSH) inequality [1]. For each choice of four numbers $a_1, a_1', a_2, a_2' \in \{-1, +1\}$, the quantity $S = \frac{1}{2}(a_2 + a_2')a_1 + \frac{1}{2}(a_2 - a_2')a_1'$ can take only the values +1 or −1. Therefore, if the four numbers are considered as realization of random variables, the expectation of S will certainly depend on the distribution of the variables but must also satisfy $|E(S)| \leqslant 1$. These are 'trivial mathematics'. But if one turns to quantum mechanics (QM), then this inequality can be violated. Indeed, consider that a is +1 if, as a result of a measurement, a spin is found along the direction $+\boldsymbol{a}$, and a is −1 if the spin is found along the direction $-\boldsymbol{a}$. This is achieved by replacing a by the operator $\boldsymbol{a} \cdot \boldsymbol{\sigma} \equiv \sigma_a$. Using this prescription for a_1, a_1', a_2 and a_2' we find that S is the expectation value of the 'Bell operator'[2]

$$B_2(\boldsymbol{a_1}, \boldsymbol{a_1'}, \boldsymbol{a_2}, \boldsymbol{a_2'}) = \tfrac{1}{2}(\sigma_{a_2} + \sigma_{a_2'}) \otimes \sigma_{a_1} + \tfrac{1}{2}(\sigma_{a_2} - \sigma_{a_2'}) \otimes \sigma_{a_1'} \tag{1}$$

where $\boldsymbol{a_1}, \boldsymbol{a_1'}, \boldsymbol{a_2}, \boldsymbol{a_2'}$ are unit vectors that will be referred to as the 'parameters' of the Bell operator. It is well known that for some choices of the parameters the highest eigenvalue of B_2 can be higher than 1: there exist some states $|\Psi\rangle$ that violate the inequality $|\langle B_2\rangle_\Psi| =$

[1] Corresponding author.

[2] Usually, the CHSH operator is written without the factor $\frac{1}{2}$ in front of it, so that the Bell's inequality is $S \leqslant 2$.

$|E(S)| \leqslant 1$. 'Trivial mathematics' fail whenever $[\sigma_{a_k}, \sigma_{a'_k}] \neq 0$, that is whenever $\boldsymbol{a_k} \neq \pm \boldsymbol{a'_k}$: in this case the 'random variables' a_k and a'_k cannot simultaneously have a precise value.

The first Bell's inequalities were derived for two two-level systems (hereafter referred to as 'qubits'). Generalizations of the Bell's inequalities have been proposed along the following lines: (i) bipartite inequalities for two n-level quantum systems [2]; (ii) bipartite inequalities using more than two parameters per system $a_1, a'_1, a''_1, \ldots$ [3]; (iii) multipartite inequalities, that is, inequalities involving more than two quantum systems [4–6].

In this paper, we consider inequalities involving an arbitrary number of qubits using two observables per qubit (the observables are obviously dichotomic). This family of inequalities has been studied in great detail independently by Werner and Wolf [7] and by Zukowski and Brukner [8]. Our present contribution consists of exhibiting explicitly the spectral decomposition of Bell's operators (section 2). Section 3 presents applications of this result.

2. Spectral decomposition of Bell operators

2.1. *Inequalities for two observables*

Consider a quantum system composed of n qubits, that is a system described by the Hilbert space $(\mathbb{C}^2)^{\otimes n}$. For each qubit k, we define two observables $A_k(0) = \sigma_{a_k}$ and $A_k(1) = \sigma_{a'_k}$, with $\boldsymbol{a_k}$ and $\boldsymbol{a'_k}$ being two vectors on the unit sphere. The set $\{\boldsymbol{a_1}, \boldsymbol{a'_1}, \ldots \boldsymbol{a_n}, \boldsymbol{a'_n}\}$ of the $2n$ unit vectors is written $\underline{\boldsymbol{a}}$. Up to normalization, any n-qubit Bell inequality[3] can be written as $\langle \mathcal{B}_n(\underline{\boldsymbol{a}}) \rangle \leqslant 1$ for a given Bell operator $\mathcal{B}_n$. The form of the Bell operator is a polynomial

$$\mathcal{B}_n(\underline{\boldsymbol{a}}) = \sum_{s \in \{0,1\}^n} \beta(s) \bigotimes_{k=1}^{n} A_k(s_k). \tag{2}$$

The coefficients $\beta(s)$ are rather arbitrary, provided that $\langle \mathcal{B}_n \rangle \leqslant 1$ is satisfied for all product states.

Of course, not every polynomial of the form (2) defines a good inequality; in the worst cases, for example, when the polynomial is simply $\sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n}$, one will find $\langle \mathcal{B}_n \rangle \leqslant 1$ for all states. The complete classification of all inequalities is due to Werner and Wolf [7]. A special role is played by the Mermin–Klyshko (MK) inequalities [4–6], whose corresponding Bell operator is defined recursively as

$$B_n(\underline{\boldsymbol{a}}) \equiv B_n = \tfrac{1}{2}(\sigma_{a_n} + \sigma_{a'_n}) \otimes B_{n-1} + \tfrac{1}{2}(\sigma_{a_n} - \sigma_{a'_n}) \otimes B'_{n-1} \tag{3}$$

where B'_n is obtained from B_n by exchanging $\boldsymbol{a}_k$ and $\boldsymbol{a}'_k$. In particular, B_2 is given by the CHSH inequality; B_3 is the operator that corresponds to the so-called Mermin's inequality [4]. For MK inequalities, the violation allowed by QM is $\langle B_n \rangle = 2^{(n-1)/2}$; no other inequality with two observables per qubit can reach such a violation [7]. More results on these operators are given in appendices A and B.

2.2. *Spectral decomposition: statement of the theorem*

We want to characterize the eigenvectors and eigenvalues of the Bell operator $\mathcal{B}_n$ defined in (2), for a given set of $2n$ unit vectors $\underline{\boldsymbol{a}}$. For this purpose, we can suppose without any loss of generality that all the unit vectors in $\underline{\boldsymbol{a}}$ lie in the (x, y) plane; physically, this amounts to saying that the axes x, y, z can be defined independently for each qubit. We will show the following theorem.

[3] From now onwards, expressions like 'all inequalities' mean 'all inequalities involving two observables per qubit'.

Theorem 1. *Let $\mathcal{B}_n$ given by (2), with $\boldsymbol{a_k} = \cos\alpha_k \boldsymbol{e_x} + \sin\alpha_k \boldsymbol{e_y}$ and $\boldsymbol{a'_k} = \cos\alpha'_k \boldsymbol{e_x} + \sin\alpha'_k \boldsymbol{e_y}$ for all $k = 1, \ldots, n$. Let $|0\rangle$, resp. $|1\rangle$, be the eigenvector of σ_z for the eigenvalue +1, resp. −1. Finally, let $\Omega = (\omega_1, \ldots, \omega_n) \in \{0, 1\}^n$ be a configuration of n zeros or ones, and $\bar{\Omega} = (\bar{\omega}_1, \ldots, \bar{\omega}_n)$ with $\bar{\omega}_k = 1 - \omega_k$ the complementary configuration. Then:*

(1) The 2^n n-qubit GHZ states, labelled by the configurations Ω, defined by

$$|\Psi_\Omega(\theta_\Omega)\rangle = \frac{1}{\sqrt{2}} (\mathrm{e}^{\mathrm{i}\theta_\Omega}|\Omega\rangle + |\bar{\Omega}\rangle) \tag{4}$$

form a basis of eigenvectors of $\mathcal{B}_n$ for some $\theta_\Omega = \theta_\Omega(\underline{\boldsymbol{a}})$.

(2) The parameter $\theta_\Omega = \theta_\Omega(\underline{\boldsymbol{a}})$ and the eigenvalue $\lambda_\Omega = \lambda_\Omega(\underline{\boldsymbol{a}})$ are calculated from a complex number $f_\Omega(\underline{\boldsymbol{a}})$:

$$\begin{aligned} &\textit{if } \arg f_\Omega \in [0, \pi[\textit{ then: } \theta_\Omega = -\arg f_\Omega - \pi \qquad \lambda_\Omega = -|f_\Omega| \\ &\textit{if } \arg f_\Omega \in [\pi, 2\pi[\textit{ then: } \theta_\Omega = -\arg f_\Omega \qquad \lambda_\Omega = |f_\Omega|. \end{aligned} \tag{5}$$

The complex number $f_\Omega(\underline{\boldsymbol{a}})$ is obtained as follows: take $\mathcal{B}_n$, and for all $k = 1, \ldots, n$ replace the operator σ_{a_k} by the complex number $\mathrm{e}^{\mathrm{i}\alpha_k}$ if $\omega_k = 0$ in Ω, or by the complex number $\mathrm{e}^{-\mathrm{i}\alpha_k}$ if $\omega_k = 1$ in Ω; and the analogue replacement for $\sigma_{a'_k}$.

About statement 1: it was noticed in [7] (V, D) that GHZ states are the states that maximally violate any inequality. This is an immediate corollary of statement 1, since for any matrix M it holds that $\max_v \langle v|M|v\rangle/\langle v|v\rangle$ is the maximal eigenvalue, obtained if and only if v is the eigenvector associated with that eigenvalue.

About statement 2: the definition of $f_\Omega(\underline{\boldsymbol{a}})$ may seem cumbersome, but a single example will clarify it. Take the CHSH operator to be given by (1). Then $f_{00} = \frac{1}{2}(\mathrm{e}^{\mathrm{i}\alpha_2} + \mathrm{e}^{\mathrm{i}\alpha'_2})\,\mathrm{e}^{\mathrm{i}\alpha_1} + \frac{1}{2}(\mathrm{e}^{\mathrm{i}\alpha_2} - \mathrm{e}^{\mathrm{i}\alpha'_2})\,\mathrm{e}^{\mathrm{i}\alpha'_1}$; f_{01} is obtained by replacing $\mathrm{e}^{\mathrm{i}\alpha_2}$ and $\mathrm{e}^{\mathrm{i}\alpha'_2}$ by their conjugates; $f_{10} = f_{01}^*$ and $f_{11} = f_{00}^*$, with z^* the conjugate of z.

The proof of the theorem is given in two steps. In the first step, we take advantage of a remarkable symmetry of the Bell operators to guess the basis (4); in the second step, direct calculation gives the explicit results (5).

2.3. First step

For a given rotation matrix $R \in SO(3)$, it is well known that one can find $U \in SU(2)$ such that $U\,\boldsymbol{a}\cdot\sigma\,U^{-1} = (R\boldsymbol{a})\cdot\sigma$. In particular, one can find U such that $U\sigma_a U^{-1} = \sigma_{-a} = -\sigma_a$. Since we are considering that all the parameters $\underline{\boldsymbol{a}}$ lie in the plane (x, y), the rotation that brings $\boldsymbol{a}$ on $-\boldsymbol{a}$ is a rotation by π around the z-axis, so that the corresponding unitary operation is $U \simeq \sigma_z$ (equality up to an arbitrary phase). We introduce the notation $U[k] = \mathbb{1} \otimes \cdots \otimes \sigma_z \otimes \cdots \otimes \mathbb{1}$, where the rotation is applied on the kth qubit. Note that $[U[k], U[l]] = 0$ for all k and l. Since $\mathcal{B}_n$ is a sum of terms like $\sigma_{a_1}\sigma_{a'_2}\ldots\sigma_{a_n}$, we have manifestly:

$$U[k]\,\mathcal{B}_n\,U[k]^{-1} = -\mathcal{B}_n \qquad \forall k \in \{1, \ldots, n\} \tag{6}$$

$$U[k]U[l]\,\mathcal{B}_n\,U[k]^{-1}U[l]^{-1} = \mathcal{B}_n \qquad \forall\, k, l \in \{1, \ldots, n\}. \tag{7}$$

These conditions depend critically on the assumption that the Bell operator is dichotomic: if we had three or more vectors for a qubit, we could not ensure that they lie in a plane. Condition (6) says that $\mathcal{B}_n$ and $-\mathcal{B}_n$ are linked by a unitary operation, hence the following:

Lemma 1. *If λ is an eigenvalue of $\mathcal{B}_n$ associated to $|\psi\rangle$, then $-\lambda$ is also an eigenvalue of $\mathcal{B}_n$. The vector $U[k]|\psi\rangle$ is eigenvector of $\mathcal{B}_n$ for the eigenvalue $-\lambda$, for all k.*

The symmetries (6) and (7) of $\mathcal{B}_n$ suggest that one should look for vectors satisfying

$$U[k]|\Psi\rangle \perp |\Psi\rangle \qquad \forall k \leqslant n \tag{8}$$

$$U[k]U[l]|\Psi\rangle = \mathrm{e}^{\mathrm{i}\gamma_{kl}}|\Psi\rangle \qquad \forall k, l \leqslant n \tag{9}$$

as good candidates for the eigenstates of $\mathcal{B}_n$; they would be the unique candidates if none of the eigenvalues of $\mathcal{B}_n$ were degenerate, but this is generally not the case (see appendix B). Let $|0\rangle$ (resp. $|1\rangle$) be the eigenstate of σ_z for the eigenvalue +1 (resp. -1). We decompose the n-qubit state $|\Psi\rangle$ on the basis of the product states of $|0\rangle$s and $|1\rangle$s: $|\Psi\rangle = \sum_{\Omega\in\{0,1\}^n} c_\Omega|\Omega\rangle$. We use condition (9) first:

$$\begin{aligned} U[k]U[l]|\Psi\rangle = \sum_\Omega (-1)^{\omega_k+\omega_l} c_\Omega|\Omega\rangle &\overset{(9)}{=} \mathrm{e}^{\mathrm{i}\gamma_{kl}} \sum_\Omega c_\Omega|\Omega\rangle\ \forall k, l \\ &\Longleftrightarrow [\mathrm{e}^{\mathrm{i}\pi(\omega_k+\omega_l)} - \mathrm{e}^{\mathrm{i}\gamma_{kl}}]\, c_\Omega = 0 \\ &\forall\, \Omega \in \{0,1\}^n \qquad \text{and} \qquad \forall\, k, l \leqslant n. \end{aligned} \tag{10}$$

Now suppose $c_\Omega \neq 0$: this implies, modulo 2π:

$$\gamma_{kl} = \pi(\omega_k + \omega_l) = \begin{cases} 0 & \text{if} \quad \omega_k = \omega_l \\ \pi & \text{if} \quad \omega_k \neq \omega_l. \end{cases} \tag{11}$$

That is, the choice of Ω for which $c_\Omega \neq 0$ determines completely the sequence of the γ_{kl}. Now, it is evident from (11) that only $\bar{\Omega}$ gives exactly the same sequence as Ω. Thus (10) means that once we have chosen Ω for which $c_\Omega \neq 0$, then $c_{\Omega'} = 0$ for all $\Omega' \neq \Omega, \bar{\Omega}$. We turn now to condition (8), that, with $U[k]|\Psi\rangle = \sum_\Omega (-1)^{\omega_k} c_\Omega|\Omega\rangle$, reads

$$\langle\Psi|U[k]\Psi\rangle = \sum_\Omega (-1)^{\omega_k}|c_\Omega|^2 \overset{(8)}{=} 0\ \forall k. \tag{12}$$

But we have proved just above that the states we are interested in are such that only c_Ω and $c_{\bar{\Omega}}$ can be different from zero. Thus (12) becomes $(-1)^{\omega_k}(|c_\Omega|^2 - |c_{\bar{\Omega}}|^2) = 0$, that is $|c_\Omega| = |c_{\bar{\Omega}}|$. We have then proved that a n-qubit state satisfies both (8) and (9) if and only if it is of the form (4) for a given $\Omega \in \{0,1\}^n$. Thus we have 2^n states, each labelled by one configuration Ω. The orthogonality requirement $\langle\Psi_\Omega(\theta_\Omega)|\Psi_{\Omega'}(\theta_{\Omega'})\rangle = \delta_{\Omega,\Omega'}$ is trivial but for $\Omega' = \bar{\Omega}$: in this case, we must require $\theta_{\bar{\Omega}} = \pi - \theta_\Omega$. This concludes the first step of the proof. Just two remarks before turning to the second step:

Remark 1. The state built on $\bar{\Omega}$ is entirely determined by the state built on Ω through

$$|\Psi_{\bar{\Omega}}(\theta_{\bar{\Omega}})\rangle \simeq |\Psi_\Omega(\theta_\Omega + \pi)\rangle \simeq U[k]|\Psi_\Omega(\theta_\Omega)\rangle. \tag{13}$$

The first equality follows from the requirement $\theta_{\bar{\Omega}} = \pi - \theta_\Omega$ by extracting $\theta_{\bar{\Omega}}$ as a global phase. As for the second equality:

$$\begin{aligned} U[k]|\Psi_\Omega(\theta_\Omega)\rangle &= \frac{1}{\sqrt{2}}(\mathrm{e}^{\mathrm{i}\theta_\Omega}(-1)^{\omega_k}|\Omega\rangle + (-1)^{\bar{\omega}_k}|\bar{\Omega}\rangle) \\ &= \frac{\mathrm{e}^{\mathrm{i}\theta_\Omega}(-1)^{\omega_k}}{\sqrt{2}}(|\Omega\rangle - \mathrm{e}^{-\mathrm{i}\theta_\Omega}|\bar{\Omega}\rangle) \simeq \frac{1}{\sqrt{2}}(\mathrm{e}^{\mathrm{i}(\pi-\theta_\Omega)}|\bar{\Omega}\rangle + |\Omega\rangle). \end{aligned}$$

Thus, another recipe to build a basis of states of the form (4) is the following: (i) for all Ω such as (say) $\omega_1 = 0$, choose θ_Ω and build the state $|\Psi(\Omega, \theta_\Omega)\rangle$; (ii) apply $U[k]$ to each of these states (or change θ_Ω to $\theta_\Omega + \pi$) to complete the set.

Remark 2. The two states built from $\Omega_0 = (0, \ldots, 0)$, namely $\frac{1}{\sqrt{2}}(\mathrm{e}^{\mathrm{i}\theta}|0\ldots0\rangle \pm |1\ldots1\rangle)$, are the only ones for which the γ_{kl} are independent of k and l; and are actually 0, with our choice of phases $U[k] = \sigma_z[k]$.

2.4. Second step

We must show that the states of the form (4) form a basis of eigenstates of $\mathcal{B}_n(\underline{a})$, that is

$$\mathcal{B}_n\,|\Psi_\Omega(\theta_\Omega)\rangle \;=\; \lambda_\Omega\,|\Psi_\Omega(\theta_\Omega)\rangle \tag{14}$$

with $\theta_\Omega = \theta_\Omega(\underline{a})$ and $\lambda_\Omega = \lambda_\Omega(\underline{a})$. Actually, we have to solve (14) only for the state built on $\Omega_0 = (0,\ldots,0)$

$$|\Psi_{\Omega_0}(\theta_{\Omega_0})\rangle \;\equiv\; |\Psi(\theta)\rangle = \frac{1}{\sqrt{2}}\,(\mathrm{e}^{\mathrm{i}\theta}|0\ldots0\rangle \,+\, |1\ldots1\rangle).$$

This is so, because one can exchange $|0\rangle$ and $|1\rangle$ by applying a unitary operation, here σ_x. Therefore by application of σ_x to the suitable qubits we can always transform any $|\Psi_\Omega\rangle$ into $|\Psi_{\Omega_0}\rangle$. Once we have the results for Ω_0, the results for Ω follow by taking the qubits k for which $\omega_k = 1$ in Ω, and replacing σ_{a_k} by $\sigma_x\sigma_{a_k}\sigma_x$, that is, replacing $(a_k)_y = \sin\alpha_k$ by $-\sin\alpha_k$, and the same for $\sigma_{a'_k}$. So the eigenvalue problem is reduced to the problem of finding λ and θ satisfying

$$\mathcal{B}_n(\mathrm{e}^{\mathrm{i}\theta}|0\ldots0\rangle + |1\ldots1\rangle) = \lambda\,(\mathrm{e}^{\mathrm{i}\theta}|0\ldots0\rangle + |1\ldots1\rangle). \tag{15}$$

Consider now one of the terms in (2), say $\sigma_{a_1}\otimes\cdots\otimes\sigma_{a_n}$: a standard calculation gives

$$\sigma_{a_1}\otimes\cdots\otimes\sigma_{a_n}(\mathrm{e}^{\mathrm{i}\theta}|0\ldots0\rangle + |1\ldots1\rangle) = \mathrm{e}^{\mathrm{i}\theta}\left(\prod_k \mathrm{e}^{\mathrm{i}\alpha_k}\right)|1\ldots1\rangle + \left(\prod_k \mathrm{e}^{-\mathrm{i}\alpha_k}\right)|0\ldots0\rangle.$$

Consequently the eigenvalue problem (15) gives

$$\mathcal{B}_n\,|\Psi(\theta)\rangle \;=\; \frac{1}{\sqrt{2}}\,(\mathrm{e}^{\mathrm{i}\theta} f\,|1\ldots1\rangle \,+\, f^*|0\ldots0\rangle) \;=\; \lambda|\Psi(\theta)\rangle \Longleftrightarrow \mathrm{e}^{\mathrm{i}\theta} f \;=\; \lambda \tag{16}$$

with $f(\underline{a}) = (\sum_s \beta(s)\prod_k \mathrm{e}^{\mathrm{i}\alpha_k(s_k)})$; for ease of notation, we write $\alpha_k(0)$ for α_k and $\alpha_k(1)$ for α'_k. The proof of theorem 1 is virtually concluded. The solution (5) follows by settling a matter of convention, since condition (16) can be written as $|f|\mathrm{e}^{\mathrm{i}(\theta+\arg(f))} = \lambda$ or as $|f|\mathrm{e}^{\mathrm{i}(\theta+\arg(f)+\pi)} = -\lambda$, in other words, a convention on θ fixes the sign of λ, this is nothing but the manifestation of (13). We choose as a convention that $\theta_\Omega \in [0,\pi[$ for all Ω; this convention is consistent with $\theta_{\bar{\Omega}} = \pi - \theta_\Omega$.

3. Applications and perspectives

3.1. On some non-maximally entangled states

In this section we study the violation of MK inequalities for a family of N-qubit states that clearly exhibit N-qubit entanglement. These states are

$$|\psi_N(\phi)\rangle = \cos\phi\,|0^N\rangle \,+\, \sin\phi\,|1^N\rangle \tag{17}$$

where we adopt the notation $|0^N\rangle = |0\ldots0\rangle$; by convention, we choose $\cos\phi \geqslant \sin\phi \geqslant 0$ i.e. $\phi \in [0, \frac{\pi}{4}]$.

In the case where $N = 2$, using Schmidt's decomposition *every* pure state can be written in the form $|\psi(\phi)\rangle = \cos\phi|00\rangle + \sin\phi|11\rangle$. It is well known that the CHSH inequality is violated by all pure entangled states [9]; in fact, using Horodeckis' theorem [10] one can calculate explicitly that $S_2 = \max_{\underline{a}}\langle B_2(\underline{a})\rangle_{\psi(\phi)} = \sqrt{1+\sin^2 2\phi}$, which is bigger than 1 unless $\phi = 0$. It is interesting to re-derive this result starting from the spectral decomposition of B_2. Consider the Bell states: $|\Phi_z^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\Psi_z^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. $|\psi(\phi)\rangle$ is a linear combination of $|\Phi_z^+\rangle$ and $|\Phi_z^-\rangle$. If we take the unit vectors $\underline{a}$ in the (x, y) plane, then $|\Phi_z^+\rangle$

and $|\Phi_z^-\rangle$ must be associated to opposite eigenvalues. But $|\Phi_z^+\rangle = |\Phi_x^+\rangle$ and $|\Phi_z^+\rangle = |\Psi_x^+\rangle$: therefore, by taking the unitary vectors in the (y, z) plane, we can construct B_2 as

$$B_2 = \lambda_1 (P_{\Phi_x^+} - P_{\Phi_x^-}) + \lambda_2 (P_{\Psi_x^+} - P_{\Psi_x^-}) = \lambda_1 (P_{\Phi_z^+} - P_{\Psi_z^+}) + \lambda_2 (P_{\Phi_z^-} - P_{\Psi_z^-}).$$

This way, the two vectors that have a non-zero overlap with $|\psi(\phi)\rangle$ are associated to the positive eigenvalues. The calculation of S_2 is not difficult, using the fact that $\lambda_1^2 + \lambda_2^2 = 2$ (see lemma 3 of appendix A) and the standard maximization

$$\max_\chi (A\cos\chi + B\sin\chi) = \sqrt{A^2 + B^2}. \tag{18}$$

We find indeed Horodecki's value. Thus, to obtain this maximal violation of CHSH we took advantage of the possibility of choosing the Bell states that are orthogonal to $|\psi(\phi)\rangle$ as the states associated to the negative eigenvalues of B_2. Now, this is precisely a characteristic of two-qubit maximally entangled states that *does not* generalize to three or more qubits. In fact, it is well known and easily verified that N-qubit GHZ states take the form $\frac{1}{\sqrt{2}}(|0^N\rangle + |1^N\rangle)$ only in one basis (up to trivial relabelling). Therefore, for $N > 2$, if we build $\mathcal{B}_N$ such that $|\mathrm{GHZ}_+\rangle = \frac{1}{\sqrt{2}}(|0^N\rangle + |1^N\rangle)$ is associated to the eigenvalue λ, then necessarily $|\mathrm{GHZ}_-\rangle = \frac{1}{\sqrt{2}}(|0^N\rangle - |1^N\rangle)$ will be associated to $-\lambda$.

We now consider $S_N = \max_{\underline{a}} \langle B_N(\underline{a})\rangle_{\psi_N(\phi)}$, with B_N a MK Bell operator, for arbitrary $N \geqslant 3$. Using $\langle 1^N|B_N|1^N\rangle = (-1)^N \langle 0^N|B_N|0^N\rangle$ we have

$$\langle B_N(\underline{a})\rangle_{\psi_N(\phi)} = f_N(\phi)\,\langle 0^N|B_N(\underline{a})|0^N\rangle + \sin 2\phi\, \mathrm{Re}\,(\langle 1^N|B_N(\underline{a})|0^N\rangle) \tag{19}$$

where $f_N(\phi) = [\cos^2\phi + (-1)^N \sin^2\phi]$, that is 1 for N even and $\cos 2\phi$ for N odd. The maximization of (19) over all possible choices of $\underline{a}$ is not evident for the following reason. We know that there are sets $\underline{a}$ that saturate the bound $\mathrm{Re}\,(\langle 1^N|B_N|0^N\rangle) = 2^{\frac{N-1}{2}}$; but for these we find $\langle 0^N|B_N|0^N\rangle = 0$. Similarly, the sets $\underline{a}$ that saturate the bound $\langle 0^N|B_N|0^N\rangle = 1$ give $\mathrm{Re}\,(\langle 1^N|B_N|0^N\rangle) = 0$. Let us try to guess the maximum of (19) using the insight provided by the spectral decomposition of B_N discussed in section 2 above. A natural first guess would be $B_N = 2^{\frac{N-1}{2}}(P_{\mathrm{GHZ}_+} - P_{\mathrm{GHZ}_-})$, that is $\mathrm{Re}\,(\langle 1^N|B_N|0^N\rangle) = 2^{\frac{N-1}{2}}$. This choice gives $S_N^{(g)}(\phi) = 2^{\frac{N-1}{2}} \sin 2\phi$. Numerical evidence suggests that this is indeed the maximum of (19) whenever $S_N(\phi) \geqslant 1$. This provides a criterion for the violation of the MK inequalities:

$$S_N(\phi) > 1 \Longleftrightarrow \sin 2\phi > 2^{-\frac{N-1}{2}} \begin{pmatrix} N = 3,4,5: & \text{numerically verified} \\ N > 5: & \text{conjectured} \end{pmatrix}. \tag{20}$$

Thus there exist *pure* entangled states that do not violate the MK inequality. Let us define ϕ_N as the value of ϕ at which $|\psi_N(\phi)\rangle$ ceases to violate the MK inequality: we have $\phi_2 = 0$, and $\sin 2\phi_N = 2^{-\frac{N-1}{2}}$ for $N \geqslant 3$, within the validity of (20). There is a clear discontinuity in the behaviour of ϕ_N between $N = 2$ and 3, as illustrated in figure 1: ϕ_N jumps from 0 for $N = 2$ to $\frac{\pi}{12}$ for $N = 3$, then starts decreasing again for higher N. This analysis suggests that the MK inequalities, and more generally the family of Bell's inequalities with two observables per qubit, may not be the 'natural' generalization of the CHSH inequality to more than two qubits. Whether a more suitable inequality exists is an open question.

To conclude this section, let us briefly come back to the problem of maximizing (19). The guess $S_N^{(g)}(\phi) = 2^{\frac{N-1}{2}} \sin 2\phi$ cannot be correct for all ϕ: in fact, in the limit of small ϕ values, $|\psi_N(\phi)\rangle$ approaches $|0^N\rangle$ and therefore $S(\phi)$ should converge to 1. To avoid this problem, we modify slightly our guess to

$$S_N^{(g)}(\phi) = \max[2^{\frac{N-1}{2}} \sin 2\phi,\ f_N(\phi)]. \tag{21}$$

Obviously $S_N \geqslant S_N^{(g)}$, since we know that $S_N^{(g)}$ can be reached. Numerical estimates for $N = 3, 4, 5$ prove that this guess is extremely good. Actually, for $N = 4, 5$ we found

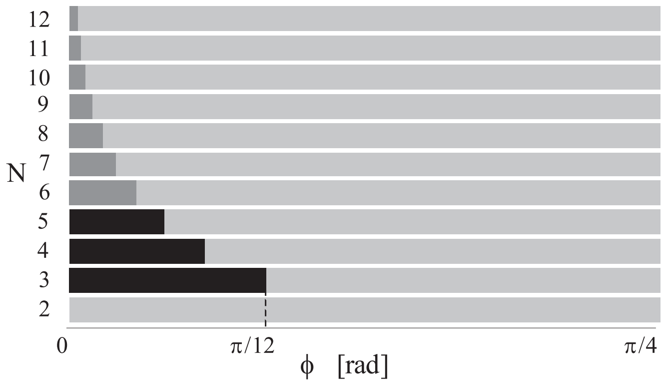

Figure 1. Ranges of ϕ for which $|\psi_N(\phi)\rangle$ violates (brighter) and does not violate (darker) the MK inequality. For $N > 5$, the result is conjectured, see (20).

$S_N(\phi) = S_N^{(g)}(\phi)$ for all ϕ to within the accuracy of the calculation; for $N = 3$, the same holds for all ϕ but a small range of values around $\bar{\phi}$ defined by $2\sin 2\bar{\phi} = \cos 2\bar{\phi}$ (the maximal difference is $S_3 - S_3^{(g)} \approx 0.002$).

3.2. Bounds on the violation of Mermin's inequality

As a second application, we show how the knowledge of the spectral decomposition of Bell operators provides bounds to estimate the violation of Mermin's inequality for any three-qubit state ρ. Some results are similar to those found independently by Zukowski and Brukner [8].

We consider a three-qubit Bell operator $\mathcal{B}_3(\underline{a})$. According to theorem 1 one can always find a basis such that its eight eigenstates are $|\Psi_{1,8}\rangle = |\Psi_{000}(0,\pi)\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)$, $|\Psi_{2,7}\rangle = |\Psi_{001}(0,\pi)\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle)$, $|\Psi_{3,6}\rangle = |\Psi_{010}(0,\pi)\rangle = \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle)$, $|\Psi_{4,5}\rangle = |\Psi_{011}(0,\pi)\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle)$. Note that the four angles θ_Ω that are unconstrained can be chosen to be 0 without loss of generality, since this amounts to a redefinition of the global phases of $|0\rangle_A$, $|0\rangle_B$ etc. Consequently in this basis

$$\begin{aligned}\mathcal{B}_3 &= \lambda_1\,(P_1 - P_8) + \lambda_2\,(P_2 - P_7) + \lambda_3\,(P_3 - P_6) + \lambda_4\,(P_4 - P_5)\\ &= \mu_{++++}\sigma_{xxx} + \mu_{-++-}\sigma_{xyy} + \mu_{-+-+}\sigma_{yxy} + \mu_{--++}\sigma_{yyx}\end{aligned}$$

with $\sigma_{xxx} = \sigma_x \otimes \sigma_x \otimes \sigma_x$ etc, and with $\mu_{s_1s_2s_3s_4} = \frac{1}{4}(s_1\lambda_1 + s_2\lambda_2 + s_3\lambda_3 + s_4\lambda_4)$. For a given three-qubit state ρ

$$\mathrm{Tr}(\mathcal{B}_3\,\rho) = \mu_{++++}t_{xxx} + \mu_{-++-}t_{xyy} + \mu_{-+-+}t_{yxy} + \mu_{--++}t_{yyx} \tag{22}$$

with the standard notation $t_{xxx} = \mathrm{Tr}(\rho\,\sigma_{xxx})$ etc. Our final purpose is to estimate $S_\rho = \max_{\underline{a}} \mathrm{Tr}(\mathcal{B}_3\,\rho)$ for any ρ. If ρ is given, one must find both the good eigenvectors and the good eigenvalues of $\mathcal{B}_3$. The optimization of the eigenvalues is performed by varying the parameters μ; we discuss it in the next paragraph for the Mermin's operator B_3. To optimize the eigenvectors means to define the axes x and y for each qubit. Note that when the basis of eigenvectors is optimized only four number t_{ijk} will come into play, thus sharpening the condition obtained by Zukowski and Brukner [8] that involved eight of these numbers.

While the system of eigenvectors is the same for all Bell operators of the form (2), the eigenvalues and their properties obviously depend on the operator that is considered. We

Table 1. S_ρ and the bounds S_ρ^+ and S_ρ^- for some three-qubit states (states not-normalized).

State	S_ρ^-	S_ρ	S_ρ^+
$\vert W\rangle = \vert 011\rangle + \vert 101\rangle + \vert 110\rangle$	1.516	1.523	1.527
$\cos\frac{\pi}{5}\vert 000\rangle + \sin\frac{\pi}{5}\vert W\rangle$	1.669	1.669	1.68
$\cos^2\frac{\pi}{5}\vert 000\rangle + \cos\frac{\pi}{5}\vert 001\rangle + \sin\frac{\pi}{5}\vert 111\rangle$	1.425	1.431	1.431
$\vert 0\rangle(\vert 00\rangle + \vert 11\rangle)$	1	$\sqrt{2}$	$\sqrt{2}$

restrict our discussion to the Mermin operator B_3 given by (3). It can then be shown that the eigenvalues must satisfy

$$\mathrm{Tr}(B_3^2) = 8 \tag{23}$$

(see lemma 3 in appendix A). This leads to $\mu_{++++}^2 + \mu_{-++-}^2 + \mu_{-+-+}^2 + \mu_{--++}^2 = 1$. Therefore, we can let $\mu_{++++} = \cos\alpha\cos\beta$, $\mu_{-++-} = \cos\alpha\sin\beta$, $\mu_{-+-+} = \sin\alpha\cos\gamma$ and $\mu_{--++} = \sin\alpha\cos\gamma$, and maximize over α, β and γ. By using thrice the maximization (18) we find

$$S_\rho \leqslant S_\rho^+ = \max_{\{x,y\}} \sqrt{t_{xxx}^2 + t_{xyy}^2 + t_{yxy}^2 + t_{yyx}^2}. \tag{24}$$

This bound would in fact be exact if there were no constraint on the eigenvalues other than (23). However, starting from the eigenvalues as they are given in statement 2 of theorem 1, one finds by inspection that the eigenvalues are bound to fulfil some other conditions, like $(\lambda_3^2 + \lambda_1^2 - 2)(\lambda_3^2 + \lambda_4^2 - 2)/(\lambda_3^2 + \lambda_2^2 - 2) = 2\sin^2(\alpha_1 - \alpha_1')$. To see that such a condition is indeed an additional constraint, we let $\lambda_2 = \lambda_3 = 1$, which is of course a possible choice. The rhs is bounded by 2, thus for the lhs not to diverge we must also have (say) $\lambda_4 = 1$; but then the condition (23) forces $\lambda_1 = 1$ too. In conclusion, if two eigenvalues are equal to 1, all the eigenvalues must be equal to 1.

Since such constraints are not easy to handle, it is interesting to provide a lower bound on S_ρ. A non-trivial one is obtained by simply choosing one possible realization of the eigenvalues, namely $\lambda_1 = \pm 2$, which due to (23) implies $\lambda_2 = \lambda_3 = \lambda_4 = 0$. This gives

$$S_\rho \geqslant S_\rho^- = \tfrac{1}{2} \max_{\{x,y\}} |t_{xxx} - t_{xyy} - t_{yxy} - t_{yyx}|. \tag{25}$$

In most cases, we still have to rely on a computer programme to calculate the bounds (24) and (25). For these bounds, the optimization bears on nine parameters (for each qubit, two parameters define the (x, y) plane and a third one fixes the axes in the plane); while a direct optimization of $\langle B_3\rangle$ bears on 12 parameters (two unit vectors per qubit).

Let us conclude by a discussion of the quality of the bounds (24) and (25) based on some examples. Consider first the family of states $|\psi_3(\phi)\rangle$ (17). From $\phi = \frac{\pi}{4}$ down to $\phi \approx \frac{\pi}{10}$ we find $S^- = S = S^+ = 2\sin 2\phi$. For smaller values of ϕ: (i) $S^- = \max(2\sin 2\phi, \cos 2\phi)$; that is, S^- corresponds to $S_3^{(g)}$ defined in (21). (ii) As we discussed earlier, the exact value S essentially follows S^-, but for small deviations. (iii) The upper bound S^+ increases again, from $S^+(\frac{\pi}{10}) \approx 1.175$ up to $S^+(0) = \sqrt{2}$. Thus this bound turns out to be too rough in the region $\phi \leqslant \frac{\pi}{12}$, where $|\psi_3(\phi)\rangle$ ceases to violate Mermin's inequality.

In table 1 we give S_ρ and the bounds S_ρ^+ and S_ρ^- for some other states. All the possible cases $S^- = S < S^+$, $S^- < S = S^+$ and $S^- < S < S^+$ are present. On all these examples, we see that at least one bound is very close, if not identical, to the exact value.

4. Conclusion

Bell's inequalities for systems of more than two qubits are the object of renewed interest, motivated by the fact that entanglement between more than two quantum systems is becoming experimentally feasible. A link between Bell's inequalities and the security of quantum communication protocols has also been stressed recently [11].

Here we focused on inequalities obtained by measuring two observables per qubit, and we gave the spectral decomposition of the corresponding operators. With these tools, we studied the violation of MK inequalities for some states that exhibit N-qubit entanglement. We proved numerically for $N = 3, 4, 5$, and we conjectured for all N, that there exist pure entangled states that do not violate these inequalities.

The authors acknowledge financial support from the Swiss FNRS and the Swiss OFES within the European project EQUIP (IST-1999-11053).

5. Appendix A. Relationships between B_n and B_n'

We derive in this appendix some properties of the MK operators B_n and B_n' that were not discussed in previous publications [5,6]. Lemma 2 was demonstrated independently and with different mathematical tools in [12].

Lemma 2. $B_n^2 = {B_n'}^2$ *for all* n.

Proof. From (3) we have

$$B_n^2 = \frac{1}{2}\,(1 + \boldsymbol{a}_n \cdot \boldsymbol{a}_n')\mathbb{1} \otimes B_{n-1}^2 + \frac{1}{2}\,(1 - \boldsymbol{a}_n \cdot \boldsymbol{a}_n')\mathbb{1} \otimes {B'}_{n-1}^2 - \frac{\mathrm{i}}{2}\,\sigma_{a_n \wedge a_n'} \otimes \left[B_{n-1},\ B_{n-1}'\right]. \tag{26}$$

${B_n'}^2$ is obtained by exchanging the primed with the non-primed objects. Therefore

$$B_n^2 - {B_n'}^2 = \boldsymbol{a}_n \cdot \boldsymbol{a}_n'\,(B_{n-1}^2 - {B'}_{n-1}^2) \propto (B_2^2 - {B_2'}^2) = 0$$

since it can be calculated explicitly that $B_2^2 = {B_2'}^2 = \mathbb{1} + \sigma_{a_2 \wedge a_2'} \otimes \sigma_{a_1 \wedge a_1'}$. □

Lemma 3. *The explicit expressions for* B_n^2 *and for the commutator* $\left[B_n,\ B_n'\right]$ *are given respectively by (29) and (30). The anticommutator is* $\{B_n, B_n'\} = 2(\boldsymbol{a}_n \cdot \boldsymbol{a}_n') \ldots (\boldsymbol{a}_1 \cdot \boldsymbol{a}_1')\,\mathbb{1}$. *As a corollary, note that* $\mathrm{Tr}(B_n^2) = 2^n$.

Proof. Lemma 2 allows us to rewrite (26) as

$$B_n^2 = \mathbb{1} \otimes B_{n-1}^2 - \frac{\mathrm{i}}{2}\,\sigma_{a_n \wedge a_n'} \otimes \left[B_{n-1},\ B_{n-1}'\right]. \tag{27}$$

Another standard calculation from (3) leads to

$$\left[B_n,\ B_n'\right] = \mathbb{1} \otimes \left[B_{n-1},\ B_{n-1}'\right] + 2\mathrm{i}\sigma_{a_n \wedge a_n'} \otimes B_{n-1}^2. \tag{28}$$

The structure of these two equations can be best seen by introducing the notations $B_n^2 \equiv P_n$, $\left[B_n,\ B_n'\right] \equiv 2\mathrm{i}Q_n$ and $\sigma_{a_n \wedge a_n'} \equiv \Sigma_n$. We have then

$$P_n = \mathbb{1} \otimes P_{n-1} + \Sigma_n \otimes Q_{n-1}$$
$$Q_n = \mathbb{1} \otimes Q_{n-1} + \Sigma_n \otimes P_{n-1}.$$

The recursive solution is a matter of patience. Using $P_2 = \mathbb{1} + \Sigma_2 \otimes \Sigma_1$ and $Q_2 = \mathbb{1} \otimes \Sigma_1 + \Sigma_2 \otimes \mathbb{1}$ we find

$$B_n^2 = {B_n'}^2 = \mathbb{1}_{2^n} + \sum_{i<j} \sigma_{a_i \wedge a_i'} \sigma_{a_j \wedge a_j'} + \sum_{i<j<k<l} \sigma_{a_i \wedge a_i'} \sigma_{a_j \wedge a_j'} \sigma_{a_k \wedge a_k'} \sigma_{a_l \wedge a_l'} + \cdots \tag{29}$$

$$\left[B_n,\ B_n'\right] = 2\mathrm{i}\left(\sum_i \sigma_{a_i \wedge a_i'} + \sum_{i<j<k} \sigma_{a_i \wedge a_i'} \sigma_{a_j \wedge a_j'} \sigma_{a_k \wedge a_k'} + \cdots\right) \tag{30}$$

where the dots indicate the sums over all products of an even, resp. an odd, number of $\sigma_{a_i \wedge a'_i}$.

Finally, the anticommutator is also found through a direct calculation from (3):

$$\{B_n, B'_n\} = \tfrac{1}{4}(2(\mathbb{1} + \{\sigma_{a_n}, \sigma_{a'_n}\} \otimes \{B_{n-1}, B'_{n-1}\}) - 2(\mathbb{1} - \{\sigma_{a_n}, \sigma_{a'_n}\} \otimes \{B_{n-1}, B'_{n-1}\})$$
$$+ \{\sigma_{a_n} + \sigma_{a'_n}, \sigma_{a_n} - \sigma_{a'_n}\} \otimes \underbrace{({B'_{n-1}}^2 - B^2_{n-1})}_{=0})$$
$$= \tfrac{1}{2}\{\sigma_{a_n}, \sigma_{a'_n}\} \otimes \{B_{n-1}, B'_{n-1}\} = (\boldsymbol{a}_n \cdot \boldsymbol{a}'_n)\mathbb{1} \otimes \{B_{n-1}, B'_{n-1}\}.$$

The conclusion follows from $\{B_2, B'_2\} = 2(\boldsymbol{a}_2 \cdot \boldsymbol{a}'_2)(\boldsymbol{a}_1 \cdot \boldsymbol{a}'_1)\, \mathbb{1}_4$. □

6. Appendix B. Some results about the maximal eigenvalue

In the main text we exhibited a set of eigenvectors of B_n that have a remarkable symmetry. But this set would lose much of this interesting feature if all eigenvalues were degenerate. Here we show that at least in one case (which is an interesting one) we can be sure that there are non-degenerate eigenvalues.

Let us first sort the eigenvalues of B_n into decreasing order: $\lambda_1 \geqslant \cdots \geqslant \lambda_{2^n}$. By virtue of lemma 1, $\lambda_k = -\lambda_{2^n-k+1}$. In particular, $\mathrm{Tr}(B_n^2) = 2(\lambda_1^2 + \lambda_2^2 + \cdots + \lambda^2_{2^{n-1}})$. Alternatively, we noticed in lemma 3 that $\mathrm{Tr}(B_n^2) = 2^n$, hence

$$\lambda_1^2 + \lambda_2^2 + \cdots + \lambda^2_{2^{n-1}} = 2^{n-1}. \tag{31}$$

In particular, if $\lambda_1 = 2^{\frac{n-1}{2}}$, then all the other eigenvalues (except of course $-\lambda_1$) are zero. In general, $\lambda_1 \geqslant 1$, where the equality holds only in the 'classical' case $\lambda_1 = \cdots = \lambda_{2^{n-1}} = -\lambda_{2^{n-1}+1} = \cdots = -\lambda_{2^n} = 1$. Equality (31) implies

$$\lambda_1^2 + \lambda_2^2 \leqslant 2^{n-1} \tag{32}$$

which leads to the following lemma.

Lemma 4. *let λ_1 and λ_2 be the two greatest eigenvalues of B_n. If $\lambda_1 > 2^{\frac{n}{2}-1}$, then it is non-degenerate, and moreover $\lambda_2 < 2^{\frac{n}{2}-1}$.*

Now, if ρ is a n-qubit state exhibiting m-party entanglement, $m \leqslant n$, it can be shown that $\langle B_n\rangle_\rho \leqslant 2^{(m-1)/2}$ [6, 12]. Thus $\lambda_1 > 2^{\frac{n}{2}-1}$ for B_n means that we have a n-qubit violation. So our last lemma reads: if the parameters $\underline{\boldsymbol{a}}$ of B_n are such that a n-qubit violation is possible, the maximal eigenvalue of B_n is non-degenerate. Actually we can prove even more as can be seen from the next lemma.

Lemma 5. *If $\lambda_1 > 2^{\frac{n}{2}-1}$, one cannot find two orthogonal states that both satisfy the condition*

$$\langle B_n\rangle_\psi > 2^{\frac{n}{2}-1}. \tag{33}$$

Due to lemma 1, the same holds for the condition $\langle B_n\rangle_\psi < -2^{\frac{n}{2}-1}$.

To prove this lemma, we determine the necessary conditions for a state $|\psi\rangle$ to satisfy (33). Let us decompose $|\psi\rangle$ on the basis of the eigenvectors of B_n: $|\psi\rangle = \sum_{k=1}^{2^n} \sqrt{p_i}\,|\Psi_i\rangle$ where $|\Psi_i\rangle$ is an eigenvector of B_n for the eigenvalue λ_i. With these notations

$$\langle\psi|B_n|\psi\rangle = \sum_{i=1}^{2^n} p_i\,\lambda_i \leqslant p_1\lambda_1 + (1-p_1)\lambda_2.$$

Therefore if $p_1\lambda_1 + (1-p_1)\lambda_2 \leqslant 2^{n/2-1}$, requirement (33) cannot be satisfied. In other terms, a necessary condition for (33) to be satisfied is

$$p_1 > \frac{2^{\frac{n}{2}-1} - \lambda_2}{\lambda_1 - \lambda_2} = \frac{1-\mu_2}{\mu_1 - \mu_2} \equiv \bar{p} \tag{34}$$

(we introduced the notation $2^{n/2-1}\mu_i = \lambda_i$ in order to show that $\bar{p}$ does not depend explicitly on the number of qubits n). It can be shown using (32) that $\frac{1}{2} < \bar{p} \leqslant 1$. The limiting case $\bar{p} = 1$ corresponds to $\lambda_1 = 2^{n/2-1}$, in which case of course (33) cannot be satisfied. The roughest criterion that we can state is therefore the following: given B_n such that $\lambda_1 > 2^{n/2-1}$, a state $|\psi\rangle$ cannot satisfy (33) if $p_1 = |\langle\Psi_1|\psi\rangle|^2 \leqslant \frac{1}{2}$. This criterion is enough to conclude the proof of lemma 5.

References

[1] Clauser J F, Horne M A, Shimony A and Holt R A 1969 *Phys. Rev. Lett.* **23** 880

[2] Garg A and Mermin N D 1982 *Phys. Rev. Lett.* **49** 901
Garg A and Mermin N D 1982 *Phys. Rev. Lett.* **49** 1294
Gisin N and Peres A 1992 *Phys. Lett.* A **162** 15

[3] Braunstein S L and Caves C M 1990 *Ann. Phys., NY* **202** 22
Zukowski M and Kaszlikowski D 1997 *Phys. Rev.* A **56** R1682
Gisin N 1999 *Phys. Lett.* A **260** 1

[4] Mermin N D 1990 *Phys. Rev. Lett.* **65** 1838

[5] Belinskii A V and Klyshko D N 1993 *Phys. Usp.* **36** 653

[6] Gisin N and Bechmann-Pasquinucci H 1998 *Phys. Lett.* A **246** 1

[7] Werner R F and Wolf M M 2001 *Preprint* quant-ph/0102024 (*Phys. Rev.* A at press)

[8] Zukowski M and Brukner C 2001 *Preprint* quant-ph/0102039

[9] Gisin N 1991 *Phys. Lett.* A **154** 201

[10] Horodecki M, Horodecki P and Horodecki M 1995 *Phys. Lett.* A **200** 340

[11] Scarani V and Gisin N 2001 *Preprint* quant-ph/0101110 (*Phys. Rev. Lett.* at press)
Scarani V and Gisin N 2001 *Preprint* quant-ph/0104016

[12] Werner R F and Wolf M M 2000 *Phys. Rev.* A **61** 062102