Optimal Distillation of a Greenberger-Horne-Zeilinger State

A. Acín,[1] E. Jané,[1] W. Dür,[2] and G. Vidal[2]

[1]*Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, E-08028 Barcelona, Spain*
[2]*Institut für Theoretische Physik, Universität Innsbruck, A-6020 Innsbruck, Austria*

(Received 18 July 2000)

We present the optimal local protocol to distill a Greenberger-Horne-Zeilinger state from a single copy of any pure state of three qubits.

Because of its relevance in quantum information theory, entanglement has been attracting considerable attention in recent years. The initial efforts, mainly devoted to acquiring a quantitative description of bipartite quantum correlations, led to the identification of the measures governing pure-state entanglement both in the asymptotic [1] and nonasymptotic [2] regimes. As a result, it is nowadays known how a bipartite system prepared in a pure state can be optimally manipulated under the restriction that only local operations on the subsystems aided with classical communication (LOCC) are allowed.

Once a relatively complete command on pure-state entanglement had been achieved for bipartite systems, efforts have moved quite recently to address the somehow more intricate case of tripartite entanglement, for which a system consisting of three two-level subsystems—that is, a three-qubit system—is the simplest scenario.

There are two distinct ways in which three qubits can be entangled [3], in the following sense. Let us identify as equivalent all pure states that can be reversibly interconverted, with some finite probability of success, when the parties are allowed to perform LOCC. Then, whereas all entangled pure states of two qubits are equivalent to the Einstein-Podolsky-Rosen (EPR) state [4], $1/\sqrt{2}\,(|00\rangle + |11\rangle)$, it turns out that truly tripartite pure-state entanglement of three qubits is either equivalent to the Greenberger-Horne-Zeilinger (GHZ) state [5],

$$|\text{GHZ}\rangle \equiv \frac{1}{\sqrt{2}}\,(|000\rangle + |111\rangle), \qquad (1)$$

or else to the W state [3], $1/\sqrt{3}\,(|001\rangle + |010\rangle + |100\rangle)$, with these two states being completely inaccessible from each other by means of LOCC.

Although it is genuinely tripartite, the entanglement of the W state only maximizes two-qubit quantum correlations [3]. As far as three-qubit correlations are concerned, the GHZ state appears as the maximally entangled state [6]: it violates Bell inequalities maximally, and it maximizes the mutual information of local measurements. It is also the only state from which an EPR state between any two chosen qubits can be obtained with certainty.

In this Letter we are concerned with the distillation of a GHZ state from an arbitrary pure state $|\psi\rangle$ of three qubits (see also [7]). We present the optimal strategy to distill a GHZ state starting from a single copy of $|\psi\rangle$. That is,

we provide the local protocol that allows the three parties to transform the state $|\psi\rangle$ into a GHZ state with the greatest *a priori* probability of success compatible with LOCC. Marginally, we also discuss the best approximate transformation [8] of $|\psi\rangle$ into $|\text{GHZ}\rangle$ by means of LOCC, which turns out to simply consist of a concatenation of local unitary transformations. Obviously, these results may be of practical interest in any situation where three parties wishing to have a GHZ state only share the state $|\psi\rangle$, and where for some reason—for instance, because they are in sufficiently distant locations—the restriction to perform only LOCC is not merely academical. From a more general perspective, several difficulties have been faced which stem from characteristic features of entanglement involving more than two subsystems, such as the nonexistence of the Schmidt decomposition (that is, from the fact that not all three-qubit states can be brought, by means of local unitary transformations, into the form $\alpha|000\rangle + \beta|111\rangle$; see [9]). In this sense, our work explores the nature of entanglement beyond the bipartite case, while providing useful tools for its study.

Let us first briefly review how, in the two-party setting, Alice and Bob can optimally distill a generic pure state of two qubits into an EPR state. The initial state can be transformed, by means of local unitary operations on Alice's and Bob's sides, into a reference state whose Schmidt decomposition is

$$\alpha|00\rangle + \beta|11\rangle, \qquad (2)$$

where $\alpha \geq \beta \geq 0$ and $\alpha^2 + \beta^2 = 1$. Then, following [1], the diagonal operator $M \equiv \frac{\beta}{\alpha}|0\rangle\langle 0| + |1\rangle\langle 1|$—corresponding to a positive operator-valued measurement (POVM) [10] on, say, Alice's part—transforms state (2) into an EPR state with probability $2\beta^2$. Finally, that such distillation protocol is optimal [11] can be interpreted in terms of the entanglement monotone $E_2 \equiv \beta^2$ [2]. Indeed, if a protocol would distill the EPR state with greater probability, this would contradict the nonincreasing character of E_2 under LOCC.

Similar steps will be followed in order to find which is the optimal distillation protocol of a GHZ state in a three-qubit system: (i) the Schmidt decomposition will be replaced with a convenient two-term product decomposition; (ii) a subclass of distillation protocols, namely, those

in which each party is allowed to perform only one POVM and only one of the overall outcomes is a GHZ state, will be discussed and optimized; (iii) the optimal of such *one successful branch protocols* (OSBP) will be proved to be the best distillation protocol by showing that the associated probability of success is an entanglement monotone [12].

Recall that a necessary and sufficient condition for the distillability of a GHZ from a three-qubit pure state $|\psi\rangle$ is that the three reduced density matrices $\rho_A \equiv \text{Tr}_{BC}|\psi\rangle\langle\psi|$, ρ_B, and ρ_C have rank 2, and that the range of $\rho_{BC} \equiv \text{Tr}_A|\psi\rangle\langle\psi|$ contains two product vectors, say, $|b_1 c_1\rangle$ and $|b_2 c_2\rangle$ [3]. Only in this case $|\psi\rangle$ admits a (unique) two-term product decomposition,

$$|\psi\rangle = \mu_1|a_1 b_1 c_1\rangle + \mu_2 e^{i\varphi}|a_2 b_2 c_2\rangle,$$
$$\mu_1 \geq \mu_2 > 0, \tag{3}$$

where $\varphi \in [0, 2\pi)$ and the normalized local vectors $|\kappa_1\rangle, |\kappa_2\rangle \in C^2$ satisfy $1 > \langle\kappa_1 | \kappa_2\rangle \geq 0$, $\kappa = a, b, c$. In its turn, a distillation protocol consists of a series of local POVMs, where the specific POVM to be performed at any time may be chosen depending on previous outcomes, the whole protocol having a tree structure. For a given branch of outcomes the initial state $|\psi\rangle$ is transformed into a final state

$$A \otimes B \otimes C|\psi\rangle, \tag{4}$$

where the local operator A collects contributions from all POVMs performed by Alice in that branch, and similarly for operators B and C. Characterizing operator A by how it transforms $|a_1\rangle$ and $|a_2\rangle$,

$$A = \alpha_1|a_1'\rangle\langle\tilde{a}_1| + \alpha_2 e^{i\varphi_a}|a_2'\rangle\langle\tilde{a}_2|, \tag{5}$$

where $\alpha_1, \alpha_2, \langle a_1' | a_2'\rangle \geq 0$ and $\{|\tilde{a}_1\rangle, |\tilde{a}_2\rangle\}$ is the biorthonormal basis to $\{|a_1\rangle, |a_2\rangle\}$, i.e., $\langle\tilde{a}_i | a_j\rangle = \delta_{ij}$, we observe that the modifications introduced by A in $|\psi\rangle$, $A \otimes \mathbb{1}_B \otimes \mathbb{1}_C|\psi\rangle = \alpha_1\mu_1|a_1' b_1 c_1\rangle + \alpha_2\mu_2 e^{i(\varphi + \varphi_a)}|a_2' b_2 c_2\rangle$, concern the weights μ_1 and μ_2, the relative phase $e^{i\varphi}$, and the local scalar product $\langle a_1 | a_2\rangle$, whereas the other two local scalar products, $\langle b_1 | b_2\rangle$ and $\langle c_1 | c_2\rangle$, remain unchanged. We can therefore readily conclude, from the uniqueness of the product decomposition (3) and the previous observation, that the only way for the resulting state (4) to be proportional to $|\text{GHZ}\rangle$ is that (i) each local operator transforms the corresponding couple of nonorthogonal, local states into an orthonormal pair, $\{|\kappa_1\rangle, |\kappa_2\rangle\} \rightarrow$

$\{|0\rangle, |1\rangle\}$, $\kappa = a, b, c$, that is,

$$A = \alpha_1|0\rangle\langle\tilde{a}_1| + \alpha_2 e^{i\varphi_a}|1\rangle\langle\tilde{a}_2|,$$
$$B = \beta_1|0\rangle\langle\tilde{b}_1| + \beta_2 e^{i\varphi_b}|1\rangle\langle\tilde{b}_2|, \tag{6}$$
$$C = \gamma_1|0\rangle\langle\tilde{c}_1| + \gamma_2 e^{i\varphi_c}|1\rangle\langle\tilde{c}_2|,$$

and that (ii) their combined effect modifies the weights μ_1 and μ_2 to be equal, $\mu_i \rightarrow \alpha_i\beta_i\gamma_i\mu_i = \sqrt{p/2}$, $i = 1, 2$ [13], where

$$p \equiv \langle\psi|A^\dagger A \otimes B^\dagger B \otimes C^\dagger C|\psi\rangle = 2(\alpha_1\beta_1\gamma_1\mu_1)^2 \tag{7}$$

is the probability that the distillation protocol follows that particular, successful branch.

We have thus seen that the three parties must act on the system in order to distill a GHZ, because each of them must orthonormalize its local couple of states. The other relevant feature of the distillation process, namely, making the relative weights equal, may be distributed in several ways among the parties.

Our OSBP for distillation consists of each of the parties performing a unique, two-outcome POVM, and it is built in such a way that after each POVM one of the two possible resulting states contains no three-partite entanglement at all, so that only one branch of the whole protocol succeeds in distilling a GHZ (see Fig. 1). In mathematical terms this implies that if, e.g., A in (6) is the successful operator in Alice's POVM, then the other operator of the local POVM, $\bar{A}$, which satisfies $A^\dagger A + \bar{A}^\dagger\bar{A} = \mathbb{1}_A$, has rank equal to 1, so that the resulting state $\bar{A} \otimes \mathbb{1}_B \otimes \mathbb{1}_C|\psi\rangle$ is a product in Alice's subsystem. Expressing the identity operator as

$$\mathbb{1}_A = \sum_{i,j} \langle a_i | a_j\rangle |\tilde{a}_i\rangle\langle\tilde{a}_j|, \tag{8}$$

and requiring that $\det[\mathbb{1}_A - A^\dagger A] = 0$, we find

$$(1 - \alpha_1^2)(1 - \alpha_2^2) = \langle a_1 | a_2\rangle^2. \tag{9}$$

Operators B and C are also accordingly constrained by

$$(1 - \beta_1^2)(1 - \beta_2^2) = \langle b_1 | b_2\rangle^2,$$
$$(1 - \gamma_1^2)(1 - \gamma_2^2) = \langle c_1 | c_2\rangle^2. \tag{10}$$

To completely characterize our protocol, we will further impose that it succeeds with the greatest possible probability over all OSBPs. The optimal OSBP probability,

$$P(\psi) \equiv \max_{\alpha_1, \beta_1, \gamma_1} 2(\alpha_1\beta_1\gamma_1\mu_1)^2, \tag{11}$$

—where the constraints $\alpha_1\beta_1\gamma_1\mu_1 = \alpha_2\beta_2\gamma_2\mu_2$ and (9) and (10) hold—reads

$$P \overset{\max}{\underset{x>0}{=}} \frac{f_1(x)f_2(x)}{2}\left(1 - \sqrt{1 - \frac{4(1 - \langle a_1 | a_2\rangle^2)}{f_1^2(x)}}\right)\left(1 - \sqrt{1 - \frac{4\mu_1^2\mu_2^2(1 - \langle b_1 | b_2\rangle^2)(1 - \langle c_1 | c_2\rangle^2)}{f_2^2(x)}}\right), \tag{12}$$

where

$$f_1(x) \equiv (x^2 + 1)/x,$$
$$f_2(x) \equiv (\mu_2^2 x^2 + 2\mu_1\mu_2\langle b_1 | b_2\rangle\langle c_1 | c_2\rangle x + \mu_1^2)/x. \tag{13}$$

The maximization in (12) involves a polynomial equation of degree 6, which in general requires numerical calcula-

tions. For illustrative purposes and later reference, we will next consider two particular situations which can be solved analytically.

Suppose, first, that the parties share the state

$$|\phi^1\rangle = \mu_1|00c_1\rangle + \mu_2|11c_2\rangle, \qquad \mu_1 \geq \mu_2 > 0, \tag{14}$$

that is, with the local states already orthogonal in Alice's and Bob's subsystems. Then the previous optimization over all OSBP leads to a maximal probability

$$P(\phi^1) = 1 - \sqrt{1 - 4\mu_1^2\mu_2^2(1 - \langle c_1 | c_2 \rangle^2)}. \quad (15)$$

This probability is 2 times the smallest eigenvalue of ρ_C, which has a decreasing behavior under LOCC. Monotonicity of this eigenvalue implies therefore that $P(\phi^1)$ is also the maximal probability for any general distilla-

tion protocol. It turns out that Claire—i.e., the party that has to orthonormalize its local states—is the only one that needs to perform a local POVM.

The second particular case concerns states of the form

$$|\phi^2\rangle = \mu_1|0b_1c_1\rangle + \mu_2|1b_2c_2\rangle, \qquad \mu_1 \geq \mu_2 > 0, \quad (16)$$

that is with orthogonal states in Alice's subsystem. The maximum probability for OSBP is

$$P(\phi^2) = (1 + 2\mu_1\mu_2\langle b_1c_1 | b_2c_2 \rangle)\left(1 - \sqrt{1 - \frac{4\mu_1^2\mu_2^2(1 - \langle b_1 | b_2 \rangle^2)(1 - \langle c_1 | c_2 \rangle^2)}{(1 + 2\mu_1\mu_2\langle b_1c_1 | b_2c_2 \rangle)^2}}\right). \quad (17)$$

Again, only Bob and Claire need to act on the system, with the corresponding POVMs satisfying

$$\frac{\beta_1^2}{\beta_2^2} = \frac{\mu_1}{\mu_2}\frac{\mu_1\langle b_1 | b_2 \rangle + \mu_2\langle c_1 | c_2 \rangle}{\mu_2\langle b_1 | b_2 \rangle + \mu_1\langle c_1 | c_2 \rangle},$$
$$\frac{\gamma_1^2}{\gamma_2^2} = \frac{\beta_2^2}{\beta_1^2}\frac{\mu_1^2}{\mu_2^2}. \quad (18)$$

So far we have analyzed the optimal distillation protocols under the constraint that only one branch leads to a GHZ. In what follows we will show that no distillation protocol can succeed with probability greater than that for OSBP, $P(\psi)$. In order to do so, we will study the behavior of $P(\psi)$ under LOCC, to conclude that it is a decreasing entanglement monotone. That is, given the state $|\psi\rangle$ and a sequence of local quantum operations that transform it into $|\psi_i\rangle$ with probability p_i, we will show that

$$P(\psi) \geq \sum_i p_i P(\psi_i), \quad (19)$$

which means that the average probability to obtain a GHZ state from $|\psi\rangle$ using several branches is not greater than when using just one branch.

Although the set of transformations LOCC is very large and one should in principle check (19) for any local protocol, we can use the fact that any such protocol decomposes into individual POVMs. Indeed, we need prove only the monotonic character of $P(\psi)$ under the most general local POVM on each subsystem. But, as a matter of fact, due to the symmetry of the problem it suffices to consider a general local POVM performed by one of the parties, say, Alice. Notice, furthermore, that any POVM can be decomposed into a sequence of two-outcome POVMs [14]. Let us then consider a two-outcome POVM with

operators $\{N_1, N_2\}$, $N_1^\dagger N_1 + N_2^\dagger N_2 = \mathbb{1}_A$, applied by Alice. With some probability p_i the resulting state will be $|\psi_i\rangle \equiv p_i^{-1/2}N_i \otimes \mathbb{1}_B \otimes \mathbb{1}_C|\psi\rangle$, and then the parties can apply the optimal OSBP, with $A_i \otimes B_i \otimes C_i$ being the corresponding successful branch [see Fig. 2(i)]. We want to show that

$$P(\psi) \geq p_1 P(\psi_1) + p_2 P(\psi_2). \quad (20)$$

Notice that the global action on Alice's side in order to distill a GHZ state can be reproduced by means of a single four-outcome POVM, namely by $\{A_1N_1, \bar{A}_1N_1, A_2N_2, \bar{A}_2N_2\}$, where $\bar{A}_i$ are the operators satisfying $A_i^\dagger A_i + \bar{A}_i^\dagger \bar{A}_i = \mathbb{1}_A$. The second and fourth operators disentangle the state. They are irrelevant for distillation, and we can join them together into some other operator R [Fig. 2(ii)]. Both operators A_1N_1 and A_2N_2, being the last transformation Alice applies to its subsystem, have to leave the local states orthonormal and therefore can be written as

$$A_iN_i = \alpha_{1,i}|0\rangle\langle\tilde{a}_1| + \alpha_{2,i}|1\rangle\langle\tilde{a}_2|. \quad (21)$$

Consequently, this three-outcome POVM can be replaced with a two-outcome POVM with operators R and

$$Q \equiv \sqrt{\alpha_{1,1}^2 + \alpha_{1,2}^2}|0\rangle\langle\tilde{a}_1| + \sqrt{\alpha_{2,1}^2 + \alpha_{2,2}^2}|1\rangle\langle\tilde{a}_2|, \quad (22)$$

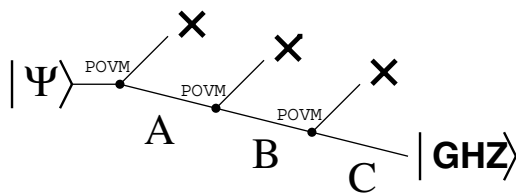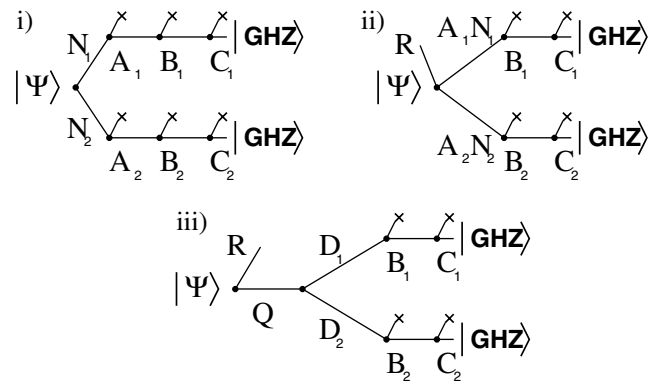followed—if the outcome corresponds to operator Q—by

FIG. 1. Scheme of a one successful branch protocol (OSBP) for distillation of a GHZ state.

FIG. 2. As far as distillation of a GHZ is concerned, these three series of conditional POVMs are equivalent [see Eqs. (20)–(24)].

a *diagonal,* two-outcome POVM [Fig. 2(iii)],

$$
D_i = \frac{\alpha_{1,i}}{\sqrt{\alpha_{1,1}^2 + \alpha_{1,2}^2}} |0\rangle\langle 0| + \frac{\alpha_{2,i}}{\sqrt{\alpha_{2,1}^2 + \alpha_{2,2}^2}} |1\rangle\langle 1|.
$$

(23)

Let $|\phi^2\rangle$ in (16) be the normalized vector after applying Q to $|\psi\rangle$. Then we can translate condition (20) into

$$
P(\phi^2) \geq q_1 P(\phi_1^2) + q_2 P(\phi_2^2),
$$

(24)

where q_i is the probability of the outcome related to D_i starting from $|\phi^2\rangle$, and $|\phi_i^2\rangle$ is the corresponding final state.

In order to finally check that (24) holds, we further notice that the action of any two-outcome POVM on a given state $|\psi\rangle$ can be reproduced by a conditional series of *balanced,* two-outcome POVMs, namely, POVMs such that, for each of them, the probability of the two outcomes is exactly $1/2$ [15]. That is, we need to analyze only a diagonal POVM where the square of the diagonal elements are $x/(2\mu_1^2)$ and $(1 - x)/(2\mu_2^2)$ for the first operator D_1, where $x \in [2\mu_1^2 - 1, 2\mu_1^2]$, and their completion to 1 for the second. Then (24) is an inequality for x that exhaustive numerical calculations have shown to saturate only for $x = \mu_1^2$, that is, when Alice acts trivially on her subsystem with $D_i = 1/\sqrt{2}\,\mathbb{1}_A$. Thus we conclude that the optimal probability for OSBP cannot be improved by any distillation protocol.

Finally, we have also considered the optimal local approximate transformation [8] of $|\psi\rangle$ into a GHZ state. That is, given the state $|\psi\rangle$ and an arbitrary local protocol which transforms it into the (possibly mixed) state ρ_i with probability p_i, we have looked for the maximal averaged fidelity between the output states ρ_i and a GHZ state,

$$
F_{\text{opt}} \equiv \max_{\text{LOCC}} \sum_i p_i \langle \text{GHZ}|\rho_i|\text{GHZ}\rangle.
$$

(25)

As we argued in the bipartite setting [8], we need to consider only final pure states $\{\psi_i, p_i\}$ due to the manifest linearity of (25) in ρ_i and the possibility of *purifying* any protocol that produces mixed states. An exhaustive numerical search shows then that the optimal approximate transformation consists of a deterministic transformation of $|\psi\rangle$ into $|\psi'\rangle$ by means of local unitary transformations, exactly as in the bipartite case.

We have addressed the optimal distillation of a GHZ state starting from a pure state of a three-qubit system. We have shown that, contrary to what happens in the bipartite case, tripartite distillation requires that each party performs at least one local POVM. This feature can be associated with the lack of Schmidt decomposition for tripartite pure states. An alternative decomposition, based on nonorthogonal product states, has proven very useful to indicate which modifications must be introduced locally in

a pure state in order to distill it into a GHZ state, and to optimize such distillation.

[1] C. H. Bennett, H. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[2] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999); D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999).

[3] W. Dür, G. Vidal, and J. I. Cirac, quant-ph/0005115.

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

[5] D. M. Greenberger, M. Horne, and A. Zeilinger, *Bell's Theorem,* edited by M. Kafatos (Kluwer, Dordrecht, 1989), p. 69.

[6] N. Gisin and H. Beschmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).

[7] O. Cohen and T. A. Brun, Phys. Rev. Lett. **84**, 5908 (2000).

[8] G. Vidal, D. Jonathan, and M. A. Nielsen, Phys. Rev. A **62**, 012304 (2000).

[9] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach, Phys. Rev. Lett. **85**, 1560 (2000); H. A. Carteret, A. Higuchi, and A. Sudbery, quant-ph/0006125.

[10] See [1] for details on how this kind of POVMs can be implemented.

[11] H.-K. Lo and S. Popescu, quant-ph/9707038.

[12] G. Vidal, J. Mod. Opt. **47**, 355 (2000).

[13] A third condition to be satisfied is that $\varphi + \varphi_a + \varphi_b + \varphi_c = 0 \bmod 2\pi$, although this can be accomplished by a simple local unitary transformation once the local states $|\kappa_i\rangle$ have been orthonormalized, and it does not affect the probability of a successful distillation.

[14] For instance, a three-outcome POVM with operators $\{E_i\}_{i=1}^3$, $\sum_i E_i^\dagger E_i = \mathbb{1}$, can be decomposed into a first two-outcome POVM with operators

$$
\{E_1, R \equiv \sqrt{E_2^\dagger E_2 + E_3^\dagger E_3}\}
$$

(26)

and a second two-outcome POVM, to be applied only if the outcome of the first POVM corresponds to the operator R, with operators $\{E_2 R^{-1}, E_3 R^{-1}\}$.

[15] Consider an *unbalanced,* two-outcome POVM $\{E_1, E_2\}$, $E_1^\dagger E_1 + E_2^\dagger E_2 = \mathbb{1}$, applied to the state $|\psi\rangle$, with $q \geq 1/2$ $[1 - q]$ being the probability of obtaining the outcome associated with E_1 $[E_2]$. Then the POVM

$$
\left\{ \frac{1}{\sqrt{2q}} E_1, R \equiv \sqrt{\frac{2q - 1}{2q} E_1^\dagger E_1 + E_2^\dagger E_2} \right\}
$$

(27)

transforms the initial state according to E_1 with probability $1/2$. If the outcome corresponds to operator R, then a new two-outcome, balanced POVM can be applied, which with probability $1/2$ will give one of the originally wished outcomes and with probability $1/2$ will require a next POVM. The whole series of balanced POVMs can easily be seen to converge towards the original unbalanced POVM.