MSc in Photonics

PHOTONICSBCN

Universitat Politècnica de Catalunya (UPC)
Universitat Autònoma de Barcelona (UAB)
Universitat de Barcelona (UB)
Institut de Ciències Fotòniques (ICFO)

http://www.photonicsbcn.eu

Master in Photonics

MASTER THESIS WORK

BEST SEPARABLE APPROXIMATION OF N-SYMMETRIC STATES

Rubén Quesada Merchán

Supervised by Dr. Anna Sanpera, (UAB)

Presented on date 27th August 2012

Registered at

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

Best separable approximation of N-symmetric states

Ruben Quesada
Universitat Autònoma de Barcelona, Bellaterra, Spain
(Dated: 26th August, 2012)

We provide a general analytical method for finding the best separable approximation of N-symmetric states.

I. INTRODUCTION

Though it is almost a century since the inception of quantum mechanics, its foundations and origin remain quite puzzling and continue to inspire intense inquiry. In particular, entanglement is one of the most intriguing properties of quantum mechanics [1] and resource of numerous applications such as quantum computation, which could surpass classical computers in some aspects [2–4], and quantum cryptography, which is expected to provide absolutely secure key distributions [5, 6].

Each of these applications by itself is worth the effort of studying entanglement and, for this reason, numerous papers have been published in the past decades about detecting and clasifying entangled states.

The principal problem arising from the study of entanglement is that of determining whether a given state is entangled or not, and is known as the *separability problem.* A formal statement of the separability problem depends upon the nature of the state. Hence, a pure state is entangled iff (if and ony if)

$$|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle, \tag{1}$$

where $|\psi_i\rangle$ are states of local subsystems. That is, a pure state is entangled if it cannot be represented as simple tensor product of its subsytem pure states (parties), otherwise it is said *separable.*

The definition of entanglement can also be extended to include *mixed states*, as follows. Mixed quantum states in which entanglement is most easily understood are states ρ_{AB} of bipartite systems in which the labels A and B corresponds to the different subsystems. Mixed states are called separable (not entangled) iff they can be written as *convex combinations* of products,

$$\rho_{AB} = \sum_i p_i \rho_{Ai} \otimes \rho_{Bi}, \tag{2}$$

where $0 \leq p_i \leq 1$ and $\sum_i p_i = 1$, ρ_A and ρ_B being mixed states of the subsystem Hilbert spaces, $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. This can be trivially extended to multipartite systems. Separable mixed states contain no entanglement, as they are by definition the mixtures of product states and so can be created by local operations and classical communications (LOCC)[14] from pure product states.

Determining if a given state, pure or mixed, is entangled or separable is not an easy task. Several separability criteria have been found, but the most versatile one is the *Positive Partial Transposition* (PPT) criterion. Peres [7] found that, for every separable state ρ, its partial transposition ρ^{T_B} (or ρ^{T_A}) is positive, where the partial transposition operation is defined as

$$\rho^{T_B}_{lm,jk} \equiv \rho_{lk,jm}, \tag{3}$$

where $\rho_{lm,jk} = \langle lm|\rho|jk\rangle$. And in a similar way for ρ^{T_A}. This necessary condition was found to be also sufficient by the Horodecki family [8], for states lying on a Hilbert space of dimension $2 \otimes 2$ or $2 \otimes 3$. It is known as the *Peres-Horodecki (PH) separability criterion*, and states that

$$\rho \text{ separable} \Rightarrow \rho^{\mathrm{T_B}} \geq 0 \tag{4}$$

$$\rho^{T_B} \geq 0 \Rightarrow \rho \text{ separable, for } \rho \in \mathbb{C}^2 \otimes \mathbb{C}^2 \text{ or } \mathbb{C}^2 \otimes \mathbb{C}^3. \tag{5}$$

The fact that the sufficient condition of the PPT criterion is valid only for such a restrictive set of states can be explained in terms of *positive maps.* A map Λ is said to be positive if for any positive operator A,

$$A \geq 0 \Rightarrow \Lambda(A) \geq 0. \tag{6}$$

Moreover, there is the definition of a *completely positive* (CP) map, which means that Λ is a CP map if the induced map

$$\Lambda_n = \mathbb{I}_n \otimes \Lambda \tag{7}$$

is positive for all n, where $\mathbb{I}_n$ is the identity map of dimension n. Of course a CP map is a positive map, but the opposite is not always true.

This leads to a separability criterion in terms of maps [8].

$$\rho \text{ separable} \Leftrightarrow (\mathbb{I} \otimes \Lambda)\rho \geq 0. \tag{8}$$

This result can be combined with the map decomposition for low dimension ($2 \otimes 2$ or $2 \otimes 3$),

$$\Lambda = \Lambda_1^{CP} + \Lambda_2^{CP} \circ T, \tag{9}$$

where Λ_i^{CP} are CP maps and T is the transposition operation. Hence, the separability criterion (8) combined with (9) is subjected to the positivity of

$$(\mathbb{I} \otimes \Lambda_1^{CP})\rho + (\mathbb{I} \otimes \Lambda_2^{CP})\rho^{T_B}. \tag{10}$$

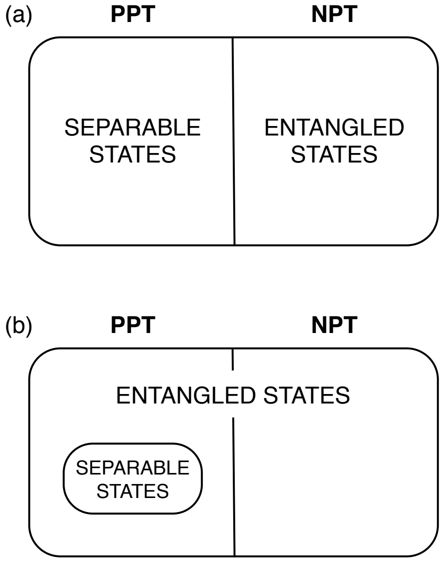

FIG. 1: Structure of entenglement for (a) states with dimension $2 \otimes 2$ or $2 \otimes 3$ (b) states with higher dimension.

Of course the positivity of (10) is commited to the positivity of ρ^{T_B} due to the definition of a CP map and the positivity of the state ρ [15]. The question arising from the PPT criterion is whether Positive Partial Transposed states (PPT states) are always separable. There exist states that are entangled but are PPT [9], thus the PPT criterion is not a sufficient condition for higher dimensions, as is shown in Figure 1. This classification has wider relevance than a mere theoretical consideration. In fact, it has been proved [10] that PPC entangled states (also called *bound entanglement* states) cannot be distilled, which means that no pure entangled states can be obtained from them by means of LOCC, and thus they cannot be used in many applications in quantum information processing. Another useful concept we will need in the following is that of *range* of ρ, defined as $\mathcal{R}(\rho) = \{|\phi\rangle : \exists|\psi\rangle : |\phi\rangle = \rho|\psi\rangle\}$. The dimension of $\mathcal{R}(\rho)$ is the rank(ρ).

A. Best Separable Approximation (BSA)

Another useful concept related with the separability of states is the known as *Lewenstein-Sanpera* (LS) decomposition. It was shown [11] that an arbitrary density matrix of a composite quantum system of finite dimension can be decomposed as

$$\rho = \lambda\rho_S + (1-\lambda)\rho_E, \tag{11}$$

where ρ_S and ρ_E are separable and entangled density matrices, respectively. In addition, if ρ is a two qubit system density matrix, the entangled part is pure, $\rho_E = |\psi\rangle\langle\psi|$. It is important to remark that, despite this decomposition is not unique, the decomposition with the maximum value of λ, called *optimal decomposition*, is in fact unique and, in this case, the separable part ρ_S receives the name of *Best Separable Approximation* (BSA). The optimal decomposition also provides a measure of the entanglement of ρ, given by

$$E(\rho) = (1-\lambda)E(\rho_E). \tag{12}$$

The existence of the BSA is confirmed by the following theorem proved in [11].

Theorem 1. *For any density matrix ρ (separable, or not) and for any set V of product vectors belonging to the range of ρ, i.e., $|e, f\rangle \in \mathcal{R}(\rho)$, there exist a separable (in general not normalized) matrix*

$$\rho_S^* = \sum_\alpha \Lambda_\alpha P_\alpha, \tag{13}$$

with all $\Lambda_\alpha \geq 0$, such that $\delta\rho = \rho - \rho_S^* \geq 0$, and that ρ_S^* provides the best separable approximation to ρ in the sense that the trace $\mathrm{Tr}(\delta\rho)$ is minimal (or, equivalently, $\mathrm{Tr}\rho_S^* \leq 1$ is maximal).

The same can be said if it is substracted the entangled part ρ_E from ρ. In this case, the BSA can be found by extracting the maximum possible entangled part ρ_E from ρ, while maintaining the separability and positivity of the diference $\rho_S^* = \rho - (1-\lambda)\rho_E$. That is, the following condition must be fullfilled

BSA Condition 1. ρ_S^* is the BSA of ρ if λ is such that, for $\epsilon > 0$,

$$\begin{array}{ll} \rho - (1-\lambda)\rho_E & \text{separable, and} \\ \rho - [1-(\lambda+\epsilon)]\rho_E & \text{not separable.} \end{array} \tag{14}$$

Or alternatively,

BSA Condition 2. ρ_S^* is the BSA of ρ if the value of λ is such that ρ_S^* is separable and $\mathrm{Tr}(\rho_S^*)$ is maximal.

There exists very few analytical methods for finding the BSA of a general state. One of them is the method given by Wellens and Kuś [12] but is only valid for 2×2 systems with rank(ρ) = 4. Now we recall some lemmas and theorems, proven in [11], which will be used later to obtain the main results of this work, and are included here for ease the reference.

Lemma 1. *Λ is maximal with respect to ρ and $P = |\psi\rangle\langle\psi|$ iff*

(a) if $|\psi\rangle \notin \mathcal{R}(\rho)$ then $\Lambda = 0$,

(b) if $|\psi\rangle \in \mathcal{R}(\rho)$ then

$$0 < \Lambda = \frac{1}{\langle\psi|\rho^{-1}|\psi\rangle}. \tag{15}$$

Lemma 2. *A pair (Λ_1, Λ_2) is maximal with respect to ρ and a pair of projectors (P_1, P_2) iff*

(a) if $|\psi_1\rangle, |\psi_2\rangle \notin \mathcal{R}(\rho)$ then $\Lambda_1 = \Lambda_2 = 0$.

(b) if $|\psi_1\rangle \notin \mathcal{R}(\rho)$, while $|\psi_2\rangle \in \mathcal{R}(\rho)$ then $\Lambda_1 = 0$, $\Lambda_2 = \langle\psi_2|\rho^{-1}|\psi_2\rangle^{-1}$.

(c) if $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{R}(\rho)$ and $\langle\phi_1|\rho^{-1}|\psi_2\rangle = 0$ then $\Lambda_i = \langle\psi_i|\rho^{-1}|\psi_i\rangle^{-1}, i = 1, 2$.

(d) if $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{R}(\rho)$ and $\langle\phi_1|\rho^{-1}|\psi_2\rangle \neq 0$ then

$$\Lambda_1 = (\langle\psi_2|\rho^{-1}|\psi_2\rangle - |\langle\psi_1|\rho^{-1}|\psi_2\rangle|)/D \tag{16}$$

$$\Lambda_2 = (\langle\psi_1|\rho^{-1}|\psi_1\rangle - |\langle\psi_1|\rho^{-1}|\psi_2\rangle|)/D, \tag{17}$$

where $D = \langle\psi_1|\rho^{-1}|\psi_1\rangle\langle\psi_2|\rho^{-1}|\psi_2\rangle - |\langle\psi_1|\rho^{-1}|\psi_2\rangle|^2$.

Theorem 2. *Given the set V of product vectors $|e, f\rangle \in \mathcal{R}(\rho)$, the matrix $\rho_S^* = \sum_\alpha \Lambda_\alpha P_\alpha$ is the BSA of ρ iff*

(a) all Λ_α are maximal with respect to $\rho_\alpha = \rho - \sum_{\alpha' \neq \alpha, \beta} \Lambda_{\alpha'} P_{\alpha'}$, and to the projector P_α

(b) all pairs $(\Lambda_\alpha, \Lambda_\beta)$ are maximal with respect to $\rho_{\alpha\beta} = \rho - \sum_{\alpha' \neq \alpha, \beta} \Lambda_{\alpha'} P_{\alpha'}$, and to the projection operators (P_α, P_β).

II. SYMMETRIC STATES

General N-symmetric states are defined as states lying in a subspace $\mathcal{S}_N$ of the Hilbert space $\mathcal{H} = \mathbb{C}^2 \otimes \overset{(N)}{\cdots} \otimes \mathbb{C}^2 \equiv (\mathbb{C}^2)^{\otimes N}$ (denoted $2^{\otimes N}$ for simplicity) with the property of being permutational invariant. It means that the interchange between any two qubits leaves the total system state unaltered.
The basis vectors are given by

$$\left|\varphi_k^N\right\rangle = \frac{1}{\sqrt{C_k^N}} \sum_\sigma \left|\sigma(1^k 0^{N-k})\right\rangle, \quad \text{for } \sigma(\mathrm{p}) \neq \sigma'(\mathrm{p}) \tag{18}$$

where $1^k 0^{N-k}$ denotes the product of k ones and $N-k$ zeroes, $1 \overset{k}{\cdots} 1 0 \overset{N-k}{\cdots} 0$; the sum is carried over every different permutation σ of $1's$ and $0's$; and $C_k^N = \binom{N}{k} = \frac{N!}{(N-k)!k!}$ is the number of ways of picking k unordered outcomes from N possibilities. It is clear that $\sigma(|\varphi_k^N\rangle) = |\varphi_k^N\rangle$, thus any state in this basis is permutational invariant.
For example, in the $N = 3$ case the vector basis $|\varphi_2^3\rangle$ is given by $\frac{1}{\sqrt{3}}(|110\rangle + |101\rangle + |011\rangle)$, which consists in every possible permutation of two 1's and one 0.
The dimension of $\mathcal{S}_N$ is $N + 1$ and it is isomorphic to $2 \otimes N$ as will be shown.
Given the basis vectors, the mixed density matrix of N-symmetric states is defined as

$$\rho = \sum_{k=0}^{N} p_k |\varphi_k^N\rangle\langle\varphi_k^N|, \tag{19}$$

where $p_k \in [0, 1]$ and $\sum_k p_k = 1$.

A. $2 \otimes 2$ symmetric states

This is the most simple non-trivial case of symmetric states from which a detailed study is worth the effort. The mixed state given by (19) with $N = 2$ is (ommiting the superindices)

$$\rho = \sum_{k=0}^{2} p_k |\varphi_k\rangle\langle\varphi_k|, \tag{20}$$

where $|\varphi_0\rangle = |00\rangle$, $|\varphi_1\rangle = |11\rangle$ and $|\varphi_2\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$, and its matrix form expressed in the computational basis is given by

$$\rho = \begin{bmatrix} p_0 & 0 & 0 & 0 \\ 0 & \frac{p_1}{2} & \frac{p_1}{2} & 0 \\ 0 & \frac{p_1}{2} & \frac{p_1}{2} & 0 \\ 0 & 0 & 0 & p_2 \end{bmatrix}. \tag{21}$$

The partial transposition of (21) with respect to the second party, ρ^{T_B}, is

$$\rho^{T_B} = \begin{bmatrix} p_0 & 0 & 0 & \frac{p_1}{2} \\ 0 & \frac{p_1}{2} & 0 & 0 \\ 0 & 0 & \frac{p_1}{2} & 0 \\ \frac{p_1}{2} & 0 & 0 & p_2 \end{bmatrix}, \tag{22}$$

whose eigenvalues are

$$\begin{aligned} \lambda_1 = \lambda_2 &= \tfrac{p_1}{2} \\ \lambda_\pm &= \tfrac{1}{2}(p_0 + p_2 \pm \sqrt{(p_1 - p_2)^2 + p_1^2}). \end{aligned} \tag{23}$$

Making use of the PH separability criterion (4-5) it is infered that the only negative eigenvalue comes from λ_-. Thus, a simple algebraic manipulation shows that

$$\rho \text{ separable} \Leftrightarrow \mathrm{p_0 p_2} \geq \left(\frac{\mathrm{p_1}}{2}\right)^2. \tag{24}$$

On the other hand, the dual condition for entanglement is stated as

$$\rho \text{ entangled} \Leftrightarrow \mathrm{p_0 p_2} < \left(\frac{\mathrm{p_1}}{2}\right)^2. \tag{25}$$

The entanglement condition (25) will be a requirement applied on ρ in order to obtain its BSA [16].
For this particular case (and for the $2\otimes2\otimes2$) the BSA can be found by subtracting the maximum possible part of entangled states ρ_E (because it is known) from ρ. From (20) can be seen that the unique entangled state is $|\varphi_2\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$, thus the entangled matrix is

$$|\varphi_2\rangle\langle\varphi_2| = \frac{1}{2} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{26}$$

Making use of BSA Condition 2, the difference $\rho_S^* = \rho - \lambda|\varphi_2\rangle\langle\varphi_2|$ is given by

$$\rho_S^* = \begin{bmatrix} p_0 & 0 & 0 & 0 \\ 0 & \frac{1}{2}p_1^{'} & \frac{1}{2}p_1^{'} & 0 \\ 0 & \frac{1}{2}p_1^{'} & \frac{1}{2}p_1^{'} & 0 \\ 0 & 0 & 0 & p_2 \end{bmatrix}, \quad (27)$$

with $p_1^{'} \equiv p_1 - 1 + \lambda$. And its partial transposition is

$$(\rho_S^*)^{T_B} = \begin{bmatrix} p_0 & 0 & 0 & \frac{1}{2}p_1^{'} \\ 0 & \frac{1}{2}p_1^{'} & 0 & 0 \\ 0 & 0 & \frac{1}{2}p_1^{'} & 0 \\ \frac{1}{2}p_1^{'} & 0 & 0 & p_2 \end{bmatrix},$$

with eigenvalues

$$\mu_1 = \mu_2 = \tfrac{1}{2}(p1 - 1 + \lambda) \quad (28)$$

$$\mu_\pm = \tfrac{1}{2}[p_0 + p_2 \pm \sqrt{(p1 - 1 + \lambda)^2 + (p_0 - p_2)^2}]. \quad (29)$$

It is easy to deduce that (28) and (29) are positive and, by virtue of the PH criterion (4-5) ρ_S^* separable, iff

$$1 - p_1 \leq \lambda \leq 1 - p_1 + 2\sqrt{p_0 p_2}. \quad (30)$$

Now being $\mathrm{Tr}\rho_\mathrm{S}^* = \mathrm{p}_0 + \mathrm{p}_1 + \mathrm{p}_2 - 1 + \lambda = \lambda$, it reaches its maximum value, within the interval (30), when

$$\begin{aligned} \lambda &= 1 - p1 + 2\sqrt{p_0 p_2} \\ &= p_0 + p_2 + 2\sqrt{p_0 p_2} \\ &= (\sqrt{p_0} + \sqrt{p_2})^2, \end{aligned} \quad (31)$$

which is ≤ 1 by (25) (and implies $\mathrm{Tr}\rho_\mathrm{S}^* \leq 1$), and gives the BSA

$$\rho_S^* = \begin{bmatrix} p_0 & 0 & 0 & 0 \\ 0 & \sqrt{p_0 p_2} & \sqrt{p_0 p_2} & 0 \\ 0 & \sqrt{p_0 p_2} & \sqrt{p_0 p_2} & 0 \\ 0 & 0 & 0 & p_2 \end{bmatrix}, \quad (32)$$

and the optimal LS decomposition

$$\rho = (\sqrt{p_0} + \sqrt{p_2})^2 \rho_S + [1 - (\sqrt{p_0} + \sqrt{p_2})^2]\rho_E. \quad (33)$$

It is interesting to notice that, as was proved in [11], for 2×2 states the entangled part of the optimal LS decomposition is pure, as $\rho_E = |\varphi_2\rangle\langle\varphi_2|$ in this case.

B. $2 \otimes 2 \otimes 2$ symmetric states

In this case, as well as in the remaining higher dimensional ones, the isomorphism $S_N \simeq 2 \otimes N$ simplifies notably the symmetric states. The basis vectors (18) for $N = 3$ are

$$|\varphi_0\rangle = |000\rangle \quad (34)$$

$$|\varphi_1\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle) \quad (35)$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{3}}(|110\rangle + |101\rangle + |011\rangle) \quad (36)$$

$$|\varphi_3\rangle = |111\rangle. \quad (37)$$

Now, with the following identifications

$$|\bar{0}\rangle = |00\rangle \quad (38)$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \quad (39)$$

$$|\bar{2}\rangle = |11\rangle, \quad (40)$$

the new basis vectors for symetric states is

$$|\varphi_0\rangle = |0\bar{0}\rangle \quad (41)$$

$$|\varphi_1\rangle = \frac{1}{\sqrt{3}}(\sqrt{2}|0\bar{1}\rangle + |1\bar{0}\rangle) \quad (42)$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{3}}(|0\bar{2}\rangle + \sqrt{2}|1\bar{1}\rangle) \quad (43)$$

$$|\varphi_3\rangle = |1\bar{2}\rangle. \quad (44)$$

In the following for simplicity the overline onto the second party will be omitted since it does not add confusion. With this new simplified basis the symmetric state (19) becomes

$$\rho = \begin{bmatrix} p_0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{2}{3}p_1 & 0 & \frac{\sqrt{2}}{3}p_1 & 0 & 0 \\ 0 & 0 & \frac{1}{3}p_2 & 0 & \frac{\sqrt{2}}{3}p_2 & 0 \\ 0 & \frac{\sqrt{2}}{3}p_1 & 0 & \frac{1}{3}p_1 & 0 & 0 \\ 0 & 0 & \frac{\sqrt{2}}{3}p_2 & 0 & \frac{2}{3}p_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & p_3 \end{bmatrix} \quad (45)$$

Its partial transposition is given by

$$\rho^{T_B} = \begin{bmatrix} p_0 & 0 & 0 & 0 & \frac{\sqrt{2}}{3}p_1 & 0 \\ 0 & \frac{2}{3}p_1 & 0 & 0 & 0 & \frac{\sqrt{2}}{3}p_2 \\ 0 & 0 & \frac{1}{3}p_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3}p_1 & 0 & 0 \\ \frac{\sqrt{2}}{3}p_1 & 0 & 0 & 0 & \frac{2}{3}p_2 & 0 \\ 0 & \frac{\sqrt{2}}{3}p_2 & 0 & 0 & 0 & p_3 \end{bmatrix}, \quad (46)$$

which has the eigenvalues

$$\mu_1 = \frac{p_1}{3} \quad (47)$$

$$\mu_2 = \frac{p_2}{3} \quad (48)$$

$$\mu_3^\pm = \frac{1}{6}\left[3p_3 + 2p_1 \pm \sqrt{8p_2^2 + (3p_3 - 2p_1)^2}\right] \quad (49)$$

$$\mu_4^\pm = \frac{1}{6}\left[3p_0 + 2p_2 \pm \sqrt{8p_1^2 + (3p_0 - 2p_2)^2}\right]. \quad (50)$$

Using the PH separability criterion (4-5), from $\mu_3^- < 0$ and $\mu_4^- < 0$ are obtained $p_2^2 > 3p_3p_1$ and $p_1^2 > 3p_0p_2$, which combined together give the entaglement conditions

$$p1 > 3p_0^{2/3}p_3^{1/3}$$
$$p2 > 3p_0^{1/3}p_3^{2/3}. \tag{51}$$

This case is quite similar to the $N = 2$, with the difference that in this case the range of ρ has at least two entangled states rather than one. We know in advance that $\mathcal{R}(\rho)$ has only two entangled states, and therefore we will need two parameters Λ_1 and Λ_2, which have to be maximized together. Again, BSA Condition 2 will be used with ρ_S^* being in this case

$$\rho_S^* = \rho - (1-\Lambda_1)|\varphi_1\rangle\langle\varphi_1| - (1-\Lambda_2)|\varphi_2\rangle\langle\varphi_2|, \tag{52}$$

where

$$|\varphi_1\rangle\langle\varphi_1| = \frac{1}{3}\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & \sqrt{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{53}$$

and

$$|\varphi_2\rangle\langle\varphi_2| = \frac{1}{3}\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \sqrt{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{54}$$

From these, the subtracted matrix (52) becomes, with the definitions $p_1^{'} \equiv p_1 - 1 + \Lambda_1$ and $p_2^{'} \equiv p_2 - 1 + \Lambda_2$,

$$\rho_S^* = \begin{bmatrix} p_0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{2}{3}p_1^{'} & 0 & \frac{\sqrt{2}}{3}p_1^{'} & 0 & 0 \\ 0 & 0 & \frac{1}{3}p_2^{'} & 0 & \frac{\sqrt{2}}{3}p_2^{'} & 0 \\ 0 & \frac{\sqrt{2}}{3}p_1^{'} & 0 & \frac{1}{3}p_1^{'} & 0 & 0 \\ 0 & 0 & \frac{\sqrt{2}}{3}p_2^{'} & 0 & \frac{2}{3}p_2^{'} & 0 \\ 0 & 0 & 0 & 0 & 0 & p_3 \end{bmatrix}. \tag{55}$$

Observing that ρ_S^* is formally identical to ρ provided that $p_1 \leftrightarrow p_1^{'}$ and $p_2 \leftrightarrow p_2^{'}$, thus the eigenvalues of $(\rho_S^*)^{T_B}$ are the same as (47-50). Positivity of $\mu_{3,4}^{\pm}$ gives the reciprocal equations of (51). These together with positivity of $\mu_{1,2}$ gives the separability conditions for $\Lambda_{1,2}$

$$1 - p_1 \le \Lambda_1 \le 1 - p_1 + 3\,p_0^{2/3}\,p_3^{1/3} \tag{56}$$
$$1 - p_2 \le \Lambda_2 \le 1 - p_2 + 3\,p_0^{1/3}\,p_3^{2/3}. \tag{57}$$

$\mathrm{Tr}\rho_S^* = \mathrm{p}_0 + \mathrm{p}_1^{'} + \mathrm{p}_2^{'} + \mathrm{p}_3 = \Lambda_1 + \Lambda_2 - 1$, from which is clear that its maximum value is achieved for the maximum value of each Λ_i subjected to (56) and (57), that is $\Lambda_1 = 1 - p_1 + 3\,p_0^{2/3}\,p_3^{1/3}$ and $\Lambda_2 = 1 - p_2 + 3\,p_0^{1/3}\,p_3^{2/3}$. Using these values the BSA ρ_S^* becomes

$$\begin{bmatrix} p_0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2p_0^{2/3}p_3^{1/3} & 0 & \sqrt{2}p_0^{2/3}p_3^{1/3} & 0 & 0 \\ 0 & 0 & p_0^{1/3}p_3^{2/3} & 0 & \sqrt{2}p_0^{1/3}p_3^{2/3} & 0 \\ 0 & \sqrt{2}p_0^{2/3}p_3^{1/3} & 0 & p_0^{2/3}p_3^{1/3} & 0 & 0 \\ 0 & 0 & \sqrt{2}p_0^{1/3}p_3^{2/3} & 0 & 2p_0^{1/3}p_3^{2/3} & 0 \\ 0 & 0 & 0 & 0 & 0 & p_3 \end{bmatrix} \tag{58}$$

The value of $\lambda = \mathrm{Tr}\rho_S^*$ is

$$\begin{aligned} \lambda &= \Lambda_1 + \Lambda_2 - 1 \\ &= 1 - p_1 - p_2 + 3p_0^{2/3}p_3^{1/3} + 3p_0^{1/3}p_3^{2/3} \\ &= p_0 + p_3 + 3p_0^{2/3}p_3^{1/3} + 3p_0^{1/3}p_3^{2/3} \\ &= (\sqrt[3]{p_0} + \sqrt[3]{p_3})^3. \end{aligned} \tag{59}$$

To sum up, the optimal LS decomposition turns out to be

$$\rho = (\sqrt[3]{p_0} + \sqrt[3]{p_3})^3 \rho_S^* + \left[1 - (\sqrt[3]{p_0} + \sqrt[3]{p_3})^3\right] \rho_E, \tag{60}$$

where ρ_E in this case is not a pure entangled state but a mixed entangled one, given by

$$\begin{aligned} \rho_E = {} & (1 - p_1 + 3\,p_0^{2/3}\,p_3^{1/3})|\varphi_1\rangle\langle\varphi_1| \\ & + (1 - p_2 + 3\,p_0^{1/3}\,p_3^{2/3})|\varphi_2\rangle\langle\varphi_2|. \end{aligned} \tag{61}$$

Notice that $0 \le \mathrm{Tr}\rho_S^* = \lambda \le 1$ due to the entanglement conditions (51). Also observe the similarity of this value of λ with that of the $N = 2$ case (31). This resemblance will turn out to be not just a coincidence but a general rule for every dimension.

III. GENERAL N-SYMMETRIC STATES

The general case of symmetric states can be simplified as in the previous examples to become a $2 \otimes N$ system. As before, the redefinition of the basis elements can be done using

$$|\bar{k}\rangle = |\varphi_k^{N-1}\rangle, \tag{62}$$

where $|\varphi_k^N\rangle$ is defined in (18). This redefinition together with the fact that

$$|\varphi_0^N\rangle = |0\rangle|\varphi_0^{N-1}\rangle \tag{63}$$
$$|\varphi_N^N\rangle = |1\rangle|\varphi_{N-1}^{N-1}\rangle \tag{64}$$
$$|\varphi_k^N\rangle = \frac{1}{\sqrt{C_k^N}}(|0\rangle\sqrt{C_k^{N-1}}|\varphi_k^{N-1}\rangle + |1\rangle\sqrt{C_{k-1}^{N-1}}|\varphi_{k-1}^{N-1}\rangle), \tag{65}$$

for $k = 1, \dots, N-1$, gives the desired basis

$$
\begin{aligned}
|\varphi_0^N\rangle &= |0\rangle|\overline{0}\rangle \\
|\varphi_N^N\rangle &= |1\rangle|\overline{N-1}\rangle \\
|\varphi_k^N\rangle &= \frac{1}{\sqrt{C_k^N}}(\sqrt{C_k^{N-1}}|0\rangle|\overline{k}\rangle + \sqrt{C_{k-1}^{N-1}}|1\rangle|\overline{k-1}\rangle).
\end{aligned}
\tag{66}
$$

Now, using the definition of C_k^N, the basis becomes unified and much simpler (the overline and the superindex N have been omitted)

$$
|\varphi_k\rangle = \sqrt{\frac{N-k}{N}}|0\rangle|k\rangle + \sqrt{\frac{k}{N}}|1\rangle|k-1\rangle, \tag{67}
$$

for $k = 0, 1, \dots, N$.

The main result of this work makes use of product states (also named product vectors), which can be found applying Lemma 2 of [13] . It states that a vector $\vec{a} = (a_{00}, \dots, a_{0(N-1)}, a_{10}, \dots, a_{(M-1)(N-1)}) \in \mathbb{C}^M \otimes \mathbb{C}^N$ is a product vector if and only if

$$
a_{ij}a_{kl} = a_{il}a_{kj}, \tag{68}
$$

for all $i, k = 0, \dots, M-1$ and $j, l = 0, \dots, N-1$, which in the particular case of symmetric states we have M=2.

First of all, we need to consider a general state $|v\rangle \in \mathcal{R}(\rho)$ which is given by

$$
|v\rangle = \sum_{k=0}^{N} m_k|\varphi_k\rangle = \frac{1}{\sqrt{N}}\begin{bmatrix} \sqrt{N}m_0 \\ \sqrt{N-1}m_1 \\ \sqrt{N-2}m_2 \\ \vdots \\ m_{N-1} \\ m_1 \\ \sqrt{2}m_2 \\ \vdots \\ \sqrt{N}m_N \end{bmatrix}. \tag{69}
$$

Hence, condition (68) becomes, for the symmetrical case (M=2), and avoiding trivial equalities (i.e. when $i = k$),

$$
a_{0j}a_{1l} = a_{0l}a_{1j}, \tag{70}
$$

for $j, l = 0, \dots, N-1$ and which applied to the state (69) means

$$
\sqrt{N-j}m_j\sqrt{l+1}m_{l+1} = \sqrt{N-l}m_l\sqrt{j+1}m_{j+1}, \tag{71}
$$

where $l \geq j+1$ to avoid duplicated expressions.
If now define equality (71) as $\mathcal{B}_{l,j+1}$, then it can be shown that $\mathcal{B}_{l,j+1} = \prod_{k=j+1}^{l} \mathcal{B}_{k,k}$. This means that only the $N-1$ equalities $\mathcal{B}_{k,k}$ for $k = 0, \dots, N$ are necessary and, since there are $N+1$ parameters m_k, we are left with only two degrees of freedom. Without loss of generality we will use m_0 and m_N as independent parameters.
Now we want to express every m_k in terms of these parameters. We have to solve, in terms of m_0 and m_N, the system given by the $\mathcal{B}_{k,k}$. After somewhat tedious but straightforward algebraic manipulations we obtain

$$
\begin{aligned}
m_k &= \sqrt{N}\sqrt{\frac{(N-1)(N-2)\cdots(N-k+1)}{2\cdot 3\cdots k}}m_0^{\frac{N-k}{N}}m_N^{\frac{k}{N}} \\
&= \sqrt{N}\sqrt{\frac{C_k^{N-1}}{N-k}}m_0^{\frac{N-k}{N}}m_N^{\frac{k}{N}}.
\end{aligned}
\tag{72}
$$

Finally, introducing (72) into (69) and defining $X^N \equiv m_0$ and $Y^N \equiv m_N$ we obtain the product vector in the computational basis, $\{|0\rangle, |1\rangle\}$,

$$
|p\rangle = \begin{bmatrix} X^N \\ \sqrt{N-1}X^{N-1}Y \\ \vdots \\ \sqrt{C_k^{N-1}}X^{N-k}Y^k \\ \vdots \\ XY^{N-1} \\ X^{N-1}Y \\ \vdots \\ \sqrt{C_j^{N-1}}X^{N-j-1}Y^{j+1} \\ \vdots \\ Y^N \end{bmatrix}. \tag{73}
$$

Expressing $|p\rangle$ in the $\{|\varphi_k\rangle\}$ basis will simplify its form and ease future calculations. Hence, decomposing $|p\rangle$ in the computational basis becomes

$$
\begin{aligned}
|p\rangle &= X^N|0\rangle|0\rangle + \cdots + X^{N-k}Y^k(\sqrt{C_k^{N-1}}|0\rangle|k\rangle \\
&\quad + \sqrt{C_{k-1}^{N-1}}|1\rangle|k-1\rangle) + \cdots + Y^N|1\rangle|N-1\rangle \qquad (74) \\
&= \sum_{k=0}^{N}\sqrt{C_k^N}X^{N-k}Y^k|\varphi_k\rangle, \qquad (75)
\end{aligned}
$$

where (66) has been used. In the following every operator will be represented in the $\{|\varphi_k\rangle\}$ basis, unless noted otherwise.
One of the key elements of this work makes use of the following map

$$
\Omega_m : X \to \omega^m X, \tag{76}
$$

where $\omega = e^{\frac{i\pi}{N}}$ is a $2N$-root of unity ($\omega^{2N} = 1$). This map induces the following transformation on the product vector $|p\rangle$

$$
\Omega_m : |p\rangle \to |p_m\rangle = \sum_{k=0}^{N}\omega^{m(N-k)}X^{N-k}Y^k|\varphi_k\rangle. \tag{77}
$$

It is important to notice that this transformation can be represented as an operator $R_m = R^m$ where R is defined (in the computational basis) as

$$R = \begin{bmatrix} \omega & \\ & 1 \end{bmatrix} \otimes \begin{bmatrix} \omega^N & & & & \\ & \omega^{N-1} & & & \\ & & \ddots & & \\ & & & \omega & \\ & & & & 1 \end{bmatrix}, \tag{78}$$

thus being obvious that $|p_m\rangle = R^m|p\rangle$ is a product state, since $|p\rangle$ is a product state. Now we define a separable state ρ_S which will turn out to be the BSA of symmetric states.

$$\rho_S \equiv \frac{1}{2N}\sum_{k=0}^{2N-1} P_k, \tag{79}$$

where $P_k = |p_k\rangle\langle p_k|$ are the projectors onto transformed product states $|p_k\rangle$ (77), thus making the state ρ_S separable by construction. This state is diagonal in the $\{|\varphi_k\rangle\}$ basis due to the relationship $\sum_{m=0}^{2N-1}\omega^{m(j-k)} = 2N\delta_{jk}$, and therefore it can be written as

$$\rho_S = \sum_{k=0}^{N} C_k^N X^{2(N-k)} Y^{2k} |\varphi_k\rangle\langle\varphi_k|. \tag{80}$$

In addition to the definition of ρ_S we will use the following prescription which will determine completely the BSA,

$$X^{2N} = p_0 \qquad Y^{2N} = p_N. \tag{81}$$

Regardless of this prescription, the notation used afterward will remain to be in terms of X and Y for simplicity. From (80) the difference $\rho - \rho_S$ is diagonal and thus we can put it as $\rho - \rho_S = \sum_{k=0}^{N} q_k |\varphi_k\rangle\langle\varphi_k|$, with the definition

$$q_k \equiv p_k - C_k^N X^{2(N-k)} Y^{2k}, \tag{82}$$

which has the remarkable property $q_0 = q_N = 0$, due to the prescription (81). Before dealing with the main theorem it is necessary before to prove some lemmas.

Lemma 3. *Given* $\rho_m \equiv \rho - \sum_{k\neq m} \Lambda_k P_k = \rho - \rho_S + \frac{1}{2N} P_m$, *then*

$$|\chi\rangle \equiv \rho_m^{-1}|p_m\rangle = \frac{2N}{b_0^*}|\varphi_0\rangle + \frac{2N}{b_N^*}|\varphi_N\rangle, \tag{83}$$

where the b_k*'s come from* $|p_m\rangle = \sum b_k|\varphi_k\rangle$.

Proof. It suffices to check that $\rho_m|\chi\rangle = |p_m\rangle$. And it is indeed what happens since $P_m|\chi\rangle = 2N|p_m\rangle$ and $q_0 = q_N = 0$ implies $(\rho - \rho_S)|\chi\rangle = 0$. □

Now we focus our attention on the following state

$$\rho_{ml} \equiv \rho - \sum_{k\neq m,l} \Lambda_k P_k \tag{84}$$

$$= \rho - \rho_S + \frac{1}{2N}(P_m + P_l) \tag{85}$$

$$= \sum q_k |\psi_k\rangle\langle\psi_k| + \frac{1}{2N}(|p_m\rangle\langle p_m| + |p_l\rangle\langle p_l|), \tag{86}$$

where $|p_m\rangle = \sum b_k|\psi_k\rangle$, $|p_l\rangle = \sum c_k|\psi_k\rangle$ and the relationship between their components is, by (77),

$$c_k = \omega^{(k-N)(m-l)} b_k \equiv \theta^{k-N} b_k, \tag{87}$$

where $\theta \equiv \omega^{m-l}$ has the property

$$\theta^N = \begin{cases} +1 & \text{if } |m-l| \text{ is even} \\ -1 & \text{if } |m-l| \text{ is odd} \end{cases}, \tag{88}$$

and trivially $|b_k|^2 = |c_k|^2$.
We also define a_k and $\bar{a}_k$ as

$$\rho_{ml}^{-1}|p_m\rangle = \sum a_k|\varphi_k\rangle \equiv |\Psi_m\rangle \tag{89}$$

$$\rho_{ml}^{-1}|p_l\rangle = \sum \bar{a}_k|\varphi_k\rangle \equiv |\Psi_l\rangle. \tag{90}$$

Using (87) and (86) we obtain that $\rho_{ml}|\psi_m\rangle = |p_m\rangle$ gives the following relationship for a_k

$$\sum_{i=0}^{N} a_i b_i^* (1 + \theta^{k-i} + \delta_{ki} P_k) = 2N, \quad k = 0,\ldots,N. \tag{91}$$

and similarly for $\rho_{ml}|\psi_l\rangle = |p_l\rangle$, giving the relationship for $\bar{a}_k$

$$\sum_{i=0}^{N} \bar{a}_i c_i^* (1 + \theta^{i-k} + \delta_{ki} P_k) = 2N, \quad k = 0,\ldots,N \tag{92}$$

with the definition

$$P_k \equiv \frac{2q_k}{|b_k|^2} = \frac{2q_k}{|c_k|^2}. \tag{93}$$

Other important equations are obtained (when $|m-l|$ is even) summing from $k=0$ to $k=N-1$ equations (91-92), giving

$$\sum_k a_k b_k^* = 2N - \sum_k a_k b_k^* P_k, \tag{94}$$

$$\sum_k \bar{a}_k c_k^* = 2N - \sum_k \bar{a}_k c_k^* P_k, \tag{95}$$

where has been used the fact that $\sum_{k=0}^{N-1}\theta^{k-i} = 0$ taking into account (88) when $|m-l|$ is even.

Lemma 4. $\rho_{ml}^{-1}|p_m\rangle = |\psi_m\rangle$, *where* $|\psi_m\rangle$ *is*

(a) if $|m-l|$ *is odd then*

$$|\psi_m\rangle = \frac{N}{b_0^*}|\varphi_0\rangle + \frac{N}{b_N^*}|\varphi_N\rangle. \tag{96}$$

(b) if $|m-l|$ is even then

$$|\psi_m\rangle = \sum a_k|\varphi_k\rangle, \quad (97)$$

with

$$a_0 = 0 \quad (98)$$

$$a_k = \frac{1}{D}\left[2(b_k - c_k)Q_k\right], \quad k \le N-1 \quad (99)$$

$$a_N = \frac{1}{b_N^* D}\left[4NQ + 2\sum_{k=1}^{N-1} b_k(b_k^* - c_k^*)Q_k\right], \quad (100)$$

where $D = 4Q + \sum_{k=1}^{N-1}\frac{4}{N}|b_k|^2 Q_k \sin^2[\frac{\pi}{2N}(m-l)k]$, $Q \equiv q_1\cdots q_{N-1}$ *and* $Q_k \equiv q_1\cdots\hat{q_k}\cdots q_{N-1}$, *and the hat over an element means that it does not appear in the equation.*

Proof. (a)

$$\rho_{ml}|\psi\rangle = \frac{1}{2N}[\left(\frac{N}{b_0^*}b_0^* + \frac{N}{b_N^*}b_N^*\right)|p_m\rangle \quad (101)$$

$$+ \underbrace{\left(\frac{N}{b_0^*}c_0^* + \frac{N}{b_N^*}c_N^*\right)}_{0}|p_l\rangle] = |p_m\rangle, \quad (102)$$

where the last expression in brackets vanishes because $\frac{c_0^*}{b_0^*} = \theta^N = -1$ (since $|m-l|$ is odd), while $\frac{c_N^*}{b_N^*} = 1$.
(b) In this case we only need to prove that the components a_k given in (98)-(100) fulfill relationship (91) for every k:

$$\frac{1}{D}\left\{2\sum_{i=0}^{N-1} b_i^*(b_i - c_i)(1+\theta^{k-i}+\delta_{ki}P_i)Q_i + \left[4NQ + 2\sum_{i=0}^{N-1} b_i(b_i^* - c_i^*)Q_i\right](1+\theta^k)\right\} \quad (103)$$

$$= \frac{1}{D}\left\{2\sum_{i=0}^{N-1}|b_i|^2(2-\theta^i-\theta^{-i})Q_i + 4NQ(1+\theta^k) + 2\sum_{i=0}^{N-1}\underbrace{|b_i|^2(1-\theta^i)\delta_{ki}P_i}_{2N(1-\theta^i)\delta_{ki}q_i} Q_i\right\} \quad (104)$$

$$= \frac{1}{D}\left\{2\sum_{i=0}^{N-1}|b_i|^2 4\sin^2\left[\frac{\pi}{2N}(m-l)i\right]Q_i + 8NQ\right\} = 2N, \ \forall k, \quad (105)$$

where have been used the definition of P_i (93), the relationship between b_k and c_k (87) keeping in mind that $\theta^N = 1$ since $|m-l|$ is even, and

$$2 - \theta^k - \theta^{-k} = 4\sin^2\left[\frac{\pi}{2N}(m-l)k\right]. \quad (106)$$

□

Lemma 5.

(i) $\sum a_k b_k^* P_k \in \mathbb{R}$.

(ii) $\sum a_k b_k^* P_k = \sum \bar{a}_k c_k^* P_k$.

Proof. Using Lemma 4 we know that $\sum_k a_k b_k^*$ is

$$\frac{1}{D}\left[2\sum b_k^*(b_k - c_k)Q_k + 4NQ + 2\sum b_k(b_k^* - c_k^*)Q_k\right]$$
$$= \frac{1}{D}\left[4NQ + 2\sum 4|b_k|^2\sin^2\left(\frac{\pi}{2N}(m-l)k\right)\right] \in \mathbb{R}.$$

Therefore, by (94) we obtain (i). To prove (ii) we begin with

$$\sum \bar{a}_k b_k^* = \langle p_m|\rho_{ml}^{-1}|p_l\rangle = \langle p_l|\rho_{ml}^{-1}|p_m\rangle^* = \sum a_k^* c_k, \quad (107)$$

which is true since ρ_{ml} is hermitian (and so is ρ_{ml}^{-1}). Combining equations (91-94) (with k=0) together with equation (94) we obtain

$$\sum a_i b_i^* \theta^{-i} = \sum a_i b_i^* P_i \quad (108)$$

$$\sum \bar{a}_i c_i^* \theta^i = \sum \bar{a}_i c_i^* P_i. \quad (109)$$

Using these results we can obtain

$$\sum \bar{a}_k b_k^* = \theta^{-N}\sum \theta^k \bar{a}_k c_k^* = \theta^{-N}\sum \bar{a}_k c_k^* P_k \quad (110)$$

$$\sum a_k^* c_k = \left(\sum a_k c_k^*\right)^* = \theta^{-N}\left(\sum a_k b_k^* P_k\right)^*. \quad (111)$$

Since the last term is real by (i), and using (107) we deduce (ii). □

Now we are ready for proving the main theorem of this work.

Theorem 3.

$$\rho_S = \frac{1}{2N}\sum_{k=0}^{2N-1} P_k \tag{112}$$

is the BSA of general N-symmetric states (19) provided that $q_k \geq 0$, where $P_k = |p_k\rangle\langle p_k|$ is obtained by the transformation $X \to \omega^k X$ of product state $|p\rangle$ (75), with $\omega = e^{\frac{i\pi}{N}}$ being a $2N$-root of unity.

Proof. The procedure to prove this theorem is to check that the conditions given in Theorem 2 for a state to be the BSA of ρ are fulfilled. The first condition states that:
(a) *all Λ_m are maximal with respect to ρ_m and P_m.*
Following Lemma 1 we need to compute $\langle p_m|\rho_m^{-1}|p_m\rangle$. Using Lemma 3 we have

$$\langle p_m|\rho_m^{-1}|p_m\rangle = \frac{N}{b_0^*}\langle p_m|\varphi_0\rangle + \frac{N}{b_N^*}\langle p_m|\varphi_N\rangle = 2N, \tag{113}$$

and therefore $\Lambda_m = \frac{1}{2N}$ for every m.

The second condition states that:
(b) *all pairs (Λ_m, Λ_l) are maximal with respect to ρ_{ml} and the projectors P_m and P_l.*
This part of the proof consists in two separate complementary parts which together give rise to the full proof. Maximality of pairs (Λ_m, Λ_l) is provided by Lemma 2, and we will separate the cases of $|m-l|$ even and odd because they involve very different complexity levels

• $|m-l|$ odd:
For this case we use part (a) of Lemma 4. Thus, we find that $\langle p_l|\rho_{ml}^{-1}|p_m\rangle = \frac{Nc_0^*}{b_0^*} + \frac{Nc_N^*}{b_N^*} = N(\theta^N + \theta^0) = 0$, since $\theta^N = -1$ for this case. Hence, to prove maximality of pairs (Λ_m, Λ_l) we have to focus on part (c) of Theorem 2. This part states that

$$\Lambda_i = \frac{1}{\langle p_i|\rho_{ml}^{-1}|p_i\rangle}, \qquad i = m, l. \tag{114}$$

Due to the symmetry between m and l it suffices to proceed with $i = m$. Trivially $\langle p_m|\rho_{ml}^{-1}|p_m\rangle = 2N$ making use of part (a) of Lemma 4.

• $|m-l|$ even:
For this case we need to follow part (d) of Theorem 3. Hence, we have to deal with

$$\Lambda_l = \frac{\langle p_m|\rho_{ml}^{-1}|p_m\rangle - |\langle p_m|\rho_{ml}^{-1}|p_l\rangle|}{\langle p_m|\rho_{ml}^{-1}|p_m\rangle\langle p_l|\rho_{ml}^{-1}|p_l\rangle - |\langle p_m|\rho_{ml}^{-1}|p_l\rangle|^2}. \tag{115}$$

Naming A the numerator and D the denominator, we have

$$A = \sum a_k b_k^* - |\sum \bar{a}_k c_k^* P_k| \tag{116}$$
$$= 2N - 2\sum a_k b_k^* P_k, \tag{117}$$

where we have used (94) and Lemma 5. On the other hand, D becomes

$$D = \left(\sum a_k b_k^*\right)\left(\sum \bar{a}_i c_i^*\right) - |\sum \bar{a}_k c_k^* P_k|^2 \tag{118}$$
$$= 4N^2 - 2N\left(\sum a_k b_k^* P_k + \sum \bar{a}_i c_i^* P_i\right) \tag{119}$$
$$= 2N\left(2N - 2\sum a_k b_k^* P_k\right) = 2NA, \tag{120}$$

using (94-95) and Lemma 5. Thus finally we arrive at

$$\Lambda_l = \frac{A}{D} = \frac{1}{2N}, \quad \forall l. \tag{121}$$

Similarly $\Lambda_m = \frac{1}{2N}$ for every m, hence completing the proof.
As a final remark, notice that the requirement $q_k \geq 0$ assures that the difference $\rho - \rho_S = \sum q_k|\varphi_k\rangle\langle\varphi_k| \geq 0$. □

The positivity condition $q_k \geq 0$ is

$$p_k - C_k^N p_0^{\frac{N-k}{N}} p_N^{\frac{k}{N}} \geq 0, \tag{122}$$

which turns out to be entanglement conditions for dimension $N = 2$ (25) and $N = 3$ (51). It is unknown, at the moment, if this is true in general for every N.
Summing up, the optimal decomposition for N-symmetric states is

$$\rho = \Lambda\bar{\rho}_S + (1-\Lambda)\rho_E, \tag{123}$$

where $\Lambda = \mathrm{Tr}(\rho_S) = (\sqrt[N]{p_0} + \sqrt[N]{p_N})^{\mathrm{N}}$ and $\bar{\rho_S}$ is normalized and defined in (79).

IV. CONCLUSIONS

In this work we have found an analytical method for finding the Best Separable Approximation of general N-symmetric states with the conditions $p_k - C_k^N p_0^{\frac{N-k}{N}} p_N^{\frac{k}{N}} \geq 0$. Also we have confirmed it for the particular cases 2×2 and $2\times 2\times 2$, which are the only ones for which the PH criterion applies.

ACKNOWLEDGMENTS

I would like to thank Anna Sanpera for the guidance and supervision of this work.

---

[1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] D. Deutsch and R. Jozsa, Proc. R. Soc. Lond. A, **439**, 553 (1992).

[3] L. K. Grover, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, ACM Press, New York, 212 (1996).
[4] P. W. Shor, SIAM Journal of Computing **26**, pp. 1484-1509 (1997).
[5] C. H. Bennet and G. Brassard, Proceedings of IEEE conference on computers, systems and signal processing, Bangalore, India, 175 (1984).
[6] V. Scarani, A. Acín, G. Ribordy and N. Gisin, Phys. Rev. Lett. **92**, 05791 (2004).
[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[8] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A, **223**, 1 (1996).
[9] P. Horodecki, Phys. Lett. A, **232**, 333 (1997).
[10] M. Horodecki, P. Horodecki and R. Horodecki, Springer Tracts in Modern Physics **173**, 151 (2001).
[11] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).
[12] T. Wellens and M. Kuś, Phys. Rev. A **64**, 052302 (2001).
[13] G. Thiang, Phys. Rev. A **82**, 012332 (2010).
[14] By local operations are meant operations which are applied only to subsytems.
[15] For a very interesting review see [10], a rigurous explanation can be found in [8].
[16] Because for a separable state the BSA is the state itself, we need a state to be entangled to be the task of obtaining the BSA non-trivial.