IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **42** (2009) 425302 (11pp) doi:10.1088/1751-8113/42/42/425302

Symmetric extendibility for a class of qudit states

Kedar S Ranade

Institut für Angewandte Physik, Technische Universität Darmstadt, Hochschulstraße 4a, D-64289 Darmstadt, Deutschland, Germany

E-mail: Kedar.Ranade@physik.tu-darmstadt.de

Received 29 June 2009, in final form 31 August 2009
Published 30 September 2009
Online at stacks.iop.org/JPhysA/42/425302

Abstract

The concept of symmetric extendibility has recently drawn attention in the context of tolerable error rates in quantum cryptography, where it can be used to decide whether quantum states shared between two parties can be purified by means of entanglement purification with one-way classical communication only. Unfortunately, at present there exists no simple general criterion to decide whether a state possesses a symmetric extension or not. In this paper, we derive criteria for symmetric extendibility within subclasses of all two-qudit states. Using these criteria, we can completely solve the problem for a two-parameter family of two-qudit states, which includes the isotropic states as a subclass.

PACS numbers: 03.67.−a, 03.67.Dd, 03.67.Hk

1. Introduction

The concept of symmetric extendibility has recently been introduced into the field of quantum cryptography as means to decide whether quantum states shared by two parties, Alice and Bob, may be purified by entanglement purification protocols using one-way classical communication only. Whereas there exist a criteria for the case of two-qubit states which can be applied in quantum cryptography [1, 2], very little is known about higher-dimensional states. The purpose of this work is to derive criteria for a subclass of all two-qudit states, which may be applied in quantum cryptography using higher-dimensional quantum systems (qudits) as carriers of information.

The outline of this paper is the following. In this section, we shall introduce the basic concepts and notation, including some remarks on the use of symmetric extendibility in quantum cryptography. We also state the Hurwitz–Sylvester criterion for positivity, on which a large part of our discussion relies. In section 2, we introduce the class of $\mathfrak{U}_2$-invariant two-qudit states, which are of interest in quantum cryptography [3, 4]; for these states we derive a criterion (theorem 1) in order to decide whether they are symmetrically extendible or not. We restrict our focus to the class of Bell-diagonal $\mathfrak{U}_2$-invariant states, which are of even

greater interest in quantum cryptography [3–5] in section 3 and simplify our criterion to find theorem 2. In a subclass of these states we use this theorem to completely solve the question of symmetric extendibility in a two-parameter family of two-qudit states, which form a superset of the isotropic states. Finally, we conclude the paper with section 4.

1.1. Definition and basic facts

We consider three d-dimensional Hilbert spaces $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}_E = \mathbb{C}^d, d \in \mathbb{N} \setminus \{1\}$ (this naming arises from Alice, Bob and Eve in quantum cryptography), each of which has a basis labeled by the elements of the ring of residue classes $\mathbb{Z}/d\mathbb{Z}$. This ring we shall identify with the numbers in $\mathbb{Z}_d := \{0, \ldots, d-1\}$, where all the operations (in particular, addition '$\oplus$' and subtraction '$\ominus$') are taken modulo d. In the following, we take a basis to be $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\} \subseteq \mathbb{C}^d$ and all sums run over $\mathbb{Z}_d$. We start with the definition of symmetric extendibility; in a more general context, it may be called $(1, 2)$-symmetric extendibility [6], but this is not within the scope of this work.

Definition 1 (Symmetric extendibility)**.** *A state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is called symmetrically extendible, if there exists a state ρ_{ABE} on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ with $\mathcal{H}_E = \mathcal{H}_B$, such that $\rho_{ABE} = \rho_{AEB}$ and $\mathrm{Tr}_E\, \rho_{ABE} = \rho_{AB}$ hold.*

Obviously all separable states have a symmetric extension, whilst no pure entangled state does. The general solution to the problem, whether a state is symmetrically extendible or not is unsolved, however, a criterion for Bell-diagonal two-qubit states is known [1] and, more generally, criteria for general two-qubit states have been investigated [2].

The use of symmetrically extendible states in quantum cryptography arises from the following observation: assume that Alice and Bob share a symmetrically extendible state ρ_{AB}. In the worst-case scenario in quantum cryptography it may happen that the attacker Eve possesses the extension, so that the overall state of the three parties is ρ_{ABE}. If Alice and Bob want to perform entanglement purification with one-way communication from Alice to Bob only, the will certainly fail, since Eve will listen to Alice's communication and do precisely the same as Bob. In other words, Bob and Eve are indistinguishable to Alice. This problem will not occur, if Bob may send information to Alice, because Eve cannot impersonate Bob. The purpose of two-way entanglement purification therefore is to convert a symmetrically extendible state into one which is not, in order to be able to use one-way purification protocols, which are normally more efficient.

To describe the problem of symmetric extendibility more explicitly, consider two general density matrices on the Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$, respectively:

$$\rho_{AB} = \sum\nolimits_{ijpq} a_{ij,pq} |ij\rangle\langle pq|, \tag{1}$$

$$\rho_{ABE} = \sum\nolimits_{ijkpqr} a_{ijk,pqr} |ijk\rangle\langle pqr|. \tag{2}$$

In order for ρ_{ABE} to be a symmetric extension of ρ_{AB} three conditions must hold:

- symmetry (between B and E): $a_{ijk,pqr} = a_{ikj,prq}$ for all $i, j, k, p, q, r \in \mathbb{Z}_d$;
- trace condition (or extension property): $\sum_{k\in\mathbb{Z}_d} a_{ijk,pqk} = a_{ij,pq}$ for all $i, j, p, q \in \mathbb{Z}_d$;
- positivity (including hermiticity): $\rho_{ABE} \geqslant 0$.

The third property guarantees that ρ_{ABE} is a quantum state, and the interplay between all three conditions causes the main problem in determining whether a symmetric extension exists or not.

1.2. The Hurwitz–Sylvester criterion

For our purposes the most useful condition for checking, whether a matrix is positive (more precisely, positive *semidefinite*), is the Hurwitz–Sylvester criterion, which we will briefly explain in the following: let $A \in \mathbb{C}^{d\times d}$ be an arbitrary matrix represented with respect to some fixed basis set, e.g. $B = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. Choosing any non-empty subset $S \subseteq B$ with cardinality $r = |S|$, we can construct the associated $r \times r$ matrix by skipping all rows and columns of A, whose basis vectors do not appear in S; the determinants of such subsets are called *principal minors* of order r, and there are altogether $2^d - 1$ principal minors of A. We now state the criterion; cf e.g. [7, p 282].

Lemma 1 (Hurwitz–Sylvester criterion for positivity)**.** *A matrix $A \in \mathbb{C}^{d\times d}$ is positive, if and only if all its principal minors are non-negative.*

This criterion is not to be confused with the better known Hurwitz–Sylvester criterion for positive-*definite* matrices, which states that a matrix is positive definite, if and only if all *leading* principal minors, that is the determinants of the d upper left submatrices, are (strictly) positive. Note in particular that lemma 1 implies that block-diagonal matrices are positive, if and only if all blocks are positive.

2. Symmetric extendibility of $\mathfrak{U}_2$-invariant states

In this section, we introduce the class of states we are interested in, the $\mathfrak{U}_2$-invariant states. These states were shown to be of interest in quantum cryptography [3], which is the main impetus for our investigation. We will derive a criterion (theorem 1) in order to decide whether there exists at least one possible symmetric extension.

2.1. Invariant states and commutants

It is yet not feasible to derive a criterion to decide whether an arbitrary two-qudit state possesses a symmetric extension or not. Thus, in order to progress we have to choose an appropriate class of these states, which should both be of physical interest and enable us to find a criterion for symmetric extendibility. A convenient way of describing states is by their commutant. Consider for example the full unitary group $\mathfrak{U}(\mathbb{C}^d \otimes \mathbb{C}^d)$ on the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ of two qudits; we may ask which states are *invariant* with respect to that group. In this particular case, Schur's lemma tells us that the only invariant state is $d^{-2}\,\mathbb{1}_{d^2}$, since $\mathfrak{U}(\mathbb{C}^d \otimes \mathbb{C}^d)$ is irreducible. More interesting examples are the states invariant with respect to $U \otimes U$ for all $U \in \mathfrak{U}(\mathbb{C}^d)$ (Werner states) or with respect to $U \otimes U^*$ for all $U \in \mathfrak{U}(\mathbb{C}^d)$ (isotropic states).

In the following, we shall focus on a superset of the set of the isotropic states. To this aim, let us define three groups:

$$\begin{aligned} \mathfrak{U}_1 &:= \left\{U \in \mathfrak{U}(\mathbb{C}^d) | U \text{ diagonal in the standard basis}\right\}, \\ \mathfrak{U}_2 &:= \{U \otimes U^* | U \in \mathfrak{U}_1\}, \\ \mathfrak{U}_3 &:= \{U \otimes U^* \otimes U^* | U \in \mathfrak{U}_1\}. \end{aligned} \tag{3}$$

We may call $\mathfrak{U}_1$ the *diagonal unitary group*; it is a maximally commutative subgroup of $\mathfrak{U}(\mathbb{C}^d)$, and any matrix $U \in \mathfrak{U}_1$ may be written in the form $U = \mathrm{diag}(w_0, w_1, \ldots, w_{d-1})$ for some system $w = (w_0, w_1, \ldots, w_{d-1}) \in \mathbb{C}^d$ of complex numbers which lie on the unit circle of $\mathbb{C}$.

2.2. *The class of* $\mathfrak{U}_2$*-invariant states*

The class of states we want to consider is the class of $\mathfrak{U}_2$-invariant states, which we describe now. Given an arbitrary $U_w = \sum_{x=0}^{d-1} w_x |x\rangle\langle x| \in \mathfrak{U}_1$ and a two-qudit state in the form of (1), we calculate

$$\begin{aligned}\big(U_w \otimes U_w^*\big)\rho_{AB} &= \textstyle\sum_{xyijpq} w_x w_y^* a_{ij,pq} |xy\rangle\, \langle xy|ij\rangle\, \langle pq| = \sum_{ijpq} w_i w_j^* a_{ij,pq} |ij\rangle\langle pq|,\\ \rho_{AB}\big(U_w \otimes U_w^*\big) &= \textstyle\sum_{xyijpq} w_x w_y^* a_{ij,pq} |ij\rangle\, \langle pq|xy\rangle\, \langle xy| = \sum_{ijpq} w_p w_q^* a_{ij,pq} |ij\rangle\langle pq|,\end{aligned} \tag{4}$$

and in order to be $\mathfrak{U}_2$-invariant, the two expressions have to be equal for all possible choices of U_w. We thus have to ensure $w_i w_j^* a_{ijpq} = w_p w_q^* a_{ijpq}$ for all $i, j, p, q \in \mathbb{Z}_d$. If $a_{ij,pq}$ is non-zero, this amounts to $w_i w_q = w_p w_j$, and since U_w is arbitrary, this can be guaranteed only if either $(i, q) = (j, p)$ or $(i, q) = (p, j)$ holds. Thus, all coefficients except those of the form $a_{ii,pp}$ or $a_{ij,ij}$ must vanish, and the matrix is diagonal up to a block of size d for the basis vectors $\{|00\rangle, |11\rangle, \ldots, |d-1, d-1\rangle\}$.

2.3. *The* $\mathfrak{U}_3$*-invariant states*

If it exists at all, a $\mathfrak{U}_2$-invariant state will have a $\mathfrak{U}_3$-invariant symmetric extension. This is because for any symmetric extension ρ_{ABE} of ρ_{AB} and any $U \in \mathfrak{U}_3$, the state $U\rho_{ABE}U^\dagger$ symmetrically extends ρ_{AB}. Averaging over the (unique) normalized Haar measure on $\mathfrak{U}_3$ will yield the invariant extension $\rho'_{ABE} = \int_{U\in\mathfrak{U}_3} U\rho_{ABE}U^\dagger \mathrm{d}U$. Algebraically spoken, if there exists an extension, it can be chosen to lie in the commutant of $\mathfrak{U}_3$ in the algebra of operators on $(\mathbb{C}^d)^{\otimes 3}$.

Since $\mathfrak{U}_3$ is commutative, it is easy to calculate its commutant, i.e. the $\mathfrak{U}_3$-invariant states. This can be done in a similar fashion as we did for $\mathfrak{U}_2$ in the previous subsection, and we find that $a_{ijk,pqr}$ may be non-zero, only if (i, q, r) and (p, j, k) are related by a permutation. This leads to a block-matrix structure in the standard basis of $(\mathbb{C}^d)^{\otimes 3}$, which we can label by the basis vectors; the blocks are

(i) blocks B_k of size $2d-1$ for basis vectors $|pkp\rangle$ and $|ppk\rangle$ for $p \neq k$ and $|kkk\rangle$;
(ii) blocks C_{ijk} of size 2 for vectors $|ijk\rangle$ and $|ikj\rangle$, i, j, k being all different;
(iii) blocks D_{ij} of size 1 for the vector $|ijj\rangle$ with $i \neq j$.

To recall our previous statements, given any extension of our state, we find an extension by setting all elements to zero, which do not lie in any of these blocks. By using the block structure it gets much easier to check positivity (see the note below lemma 1).

2.4. *The trace conditions*

Any two-qudit state can be written as $\rho_{AB} = \sum_{ij,pq} a_{ij,pq} |ij\rangle\langle pq|$; an extension will then have the form $\rho_{ABE} = \sum_{ijk,pqr} a_{ijk,pqr} |ijk\rangle\langle pqr|$, and we have to determine the coefficients $a_{ijk,pqr}$. In the case $k = r$ they have to obey certain trace conditions, and we want to check where these coefficients $a_{ijk,pqk}$ lie. We consider the two cases of nonzero coefficients of ρ_{AB}:

(i) $a_{ii,pp}$: the relevant coefficients $a_{iik,ppk}$ lie in the blocks B_k;
(ii) $a_{ij,ij}$: the relevant coefficients $a_{ijk,ijk}$ are the diagonal elements of all blocks.

The remaining coefficients $a_{ij,pq}$ are zero due to the $\mathfrak{U}_2$-invariance, and we set $a_{ijk,pqk} := 0$, since they lie outside of our block structure. We note that the off-diagonal elements $a_{ijk,ikj}$ and $a_{ikj,ijk}$ of C_{ijk} can be set to zero, since they do not appear in the trace and according to lemma 1 any other choice may only harm positivity of ρ_{ABE}.

2.5. Symmetry and the reduction of B_k to B'_k

Apart from the trace condition we still have to fulfil the symmetry $a_{ijk,pqr} = a_{ikj,prq}$. In the case of the blocks D_{ij} nothing has to be done, and for C_{ijk} we note that it is a multiple of the 2×2 unit matrix. Let us therefore focus on the blocks B_k.

Each block B_k is constructed for the basis vectors $|ppk\rangle$ and $|pkp\rangle$ for $k \neq p$ and the exceptional element $|kkk\rangle$. By symmetry $a_{iik,ppk} = a_{iki,pkp}$ and $a_{iik,pkp} = a_{iki,ppk}$ hold; whilst the first-mentioned elements appear in the trace condition, the latter do not. We now choose $a_{iik,pkp} := a_{iik,ppk}$ and show that this is not a restriction. Let B'_k be the $d \times d$ submatrix of B_k constructed for the basis vectors $|ppk\rangle$ (where $k = p$ is possible).

Lemma 2 (Equivalence of positivity of B_k and B'_k)**.** *Either B_k and B'_k are both positive semidefinite or none of them is.*

Proof. If B_k is positive definite, then so is its submatrix B'_k. Assuming that B'_k is positive semidefinite, we choose an arbitrary principal minor of B_k. If it is constructed by using a pair $|ppk\rangle$ and $|pkp\rangle$, it is zero due to our choice of the elements $a_{iik,pkp}$; if not, we can replace all $|pkp\rangle$ by $|ppk\rangle$ to yield a submatrix of B'_k. Positivity is thus ensured by lemma 1. □

Since the elements $a_{iik,pkp}$ do not appear in B'_k, any other choice may only harm positivity. Furthermore, by this reduction, we got rid of the symmetry constraint, which is now implicitly hidden in the matrices.

2.6. Building up the matrices B'_k

We now want to explicitly construct positive matrices B'_k. For shortness, let us denote $\lambda_{ijk} := a_{ijk,ijk}$ and $\lambda_{ij} := a_{ij,ij}$ for the diagonal elements; the symmetry and the second trace condition then read $\lambda_{ijk} = \lambda_{ikj}$ and $\sum_k \lambda_{ijk} = \lambda_{ij}$. For fixed $i \in \mathbb{Z}_d$, we can write a scheme, which is symmetric and consists of non-negative entries:

k : column index j : row index	0	1	...	i	...	$d-1$	row sum
0	λ_{i00}	λ_{i01}	...	λ_{i0i}	...	$\lambda_{i,0,d-1}$	λ_{i0}
1	λ_{i10}	λ_{i11}	...	λ_{i1i}	...	$\lambda_{i,1,d-1}$	λ_{i1}
$\vdots$	$\vdots$	$\vdots$	$\ddots$		$\vdots$	$\vdots$	$\vdots$
i	λ_{ii0}	λ_{ii1}	...	λ_{iii}	...	$\lambda_{i,i,d-1}$	λ_{ii}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$d-1$	$\lambda_{i,d-1,0}$	$\lambda_{i,d-1,1}$	...	$\lambda_{i,d-1,i}$	...	$\lambda_{i,d-1,d-1}$	$\lambda_{i,d-1}$
column sum	λ_{i0}	λ_{i1}	...	λ_{ii}	...	$\lambda_{i,d-1}$	

The elements on the "cross" defined by $i = j$ or $i = k$ lie in the blocks B_k, the remaining diagonal entries in blocks D_{ij} and all other in blocks C_{ijk}. The second trace condition fixes the sum of each row and each column.

Given such a scheme, positivity has to be ensured within the blocks B'_k only. If there exists a scheme which fulfils all criteria and produces positive B'_k, there exists a scheme, where C_{ijk} vanish: if some $\lambda_{ijk} =: x \geqslant 0$, by symmetry $\lambda_{ikj} = x$ holds. Substituting $\lambda'_{ijj} := \lambda_{ijj} + x$, $\lambda'_{ikk} := \lambda_{ikk} + x$ and $\lambda'_{ijk} := \lambda'_{ikj} := 0$, the trace conditions are still fulfilled, $C_{ijk} = 0$ and the diagonal elements of B'_k remain unaffected.

We can thus arbitrarily choose the diagonal entries of the matrices B'_k between zero and their maximum value, since D_{ij}, i.e. the entries $\lambda_{ijj} := \lambda_{ij} - \lambda_{iij}$ will absorb the remaining

value to fulfil the trace condition. The only thing we have to take care of is $\lambda_{iik} \leqslant \lambda_{ik}$ for all $i, k \in \mathbb{Z}_d$, since the first trace condition ensures $\sum_{p\in\mathbb{Z}_d} \lambda_{ppk} = \lambda_{pp}$ for all $k \in \mathbb{Z}_d$.

2.7. Reformulation of the trace condition and the main theorem

The matrix B'_k is constructed with respect to the basis vectors $|ppk\rangle$ for $p \in \mathbb{Z}_d$, where we now consider this particular ordering. Summing up all matrices B'_k yields

$$\sum\nolimits_{k=0}^{d-1} B'_k = \Big(\sum\nolimits_k a_{iik,ppk}\Big)_{i,p=0}^{d-1} = (a_{ii,pp})_{i,p=0}^{d-1} =: \tilde{B} \tag{5}$$

according to the first trace condition, and as a submatrix of ρ_{AB}, it is always positive. Skipping the primes in B'_k, we have altogether shown the following theorem.

Theorem 1 (Symmetric extendibility of $\mathfrak{U}_2$-invariant states)**.** *A $\mathfrak{U}_2$-invariant state $\rho_{AB} = \sum_{ijpq} a_{ij,pq}|ij\rangle\langle pq|$ is symmetrically extendible, if and only if the matrix $\tilde{B} = (a_{ii,pp})_{i,p=0}^{d-1} \in \mathbb{C}^{d\times d}$ can be decomposed into the sum of d positive matrices $B_k = (a_{iik,ppk})_{i,p=0}^{d-1} \in \mathbb{C}^{d\times d}$ for $k \in \mathbb{Z}_d$, such that their diagonal elements obey the inequalities $a_{iik,iik} \leqslant a_{ik,ik}$ for all $i, k \in \mathbb{Z}_d$.*

In general, this condition is still difficult to check, however, it is sufficiently appropriate for calculating bounds for quantum-cryptographic protocols [8], and we will use it as a starting point for the following section.

Since the sum of positive matrices is positive, we can always enlarge the diagonal elements of a positive matrix without changing its positivity. Ignoring for the moment the trace conditions, we could set the diagonal elements of all B_k to their maximum values. Considering only the non-negativity of all principal minors constructed of 2×2 submatrices, we find the following corollary.

Corollary 1 (Necessary condition for symmetric extendibility)**.** *A $\mathfrak{U}_2$-invariant symmetrically extendible state fulfils $|a_{ii,pp}| \leqslant \sum_{k=0}^{d-1} \sqrt{a_{ik,ik}a_{pk,pk}}$ for all $i, p \in \mathbb{Z}_d$.*

3. Bell-diagonal states

An important subset of all two-qudit states is the class of (generalized) Bell-diagonal states. We define the Bell basis of the Hilbert space $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$ by

$$|\Psi_{lm}\rangle := d^{-1/2} \sum\nolimits_{k=0}^{d-1} z^{lk}|k\rangle|k \ominus m\rangle, \qquad l, m \in \mathbb{Z}_d, \tag{6}$$

where $z := \exp\left(\frac{2\pi \mathrm{i}}{d}\right)$ is the principal value of the dth root of unity. The Bell-diagonal states are the convex combinations of the associated density matrices and can be written in the form

$$\rho_{AB} = \sum\nolimits_{l,m=0}^{d-1} A_{lm}|\Psi_{lm}\rangle\langle\Psi_{lm}|, \tag{7}$$

where $A_{lm} \geqslant 0$ and $\sum_{lm} A_{lm} = 1$. The coefficient system $(A_{lm})_{l,m=0}^{d-1}$ thus defines a joint probability distribution, and we write $A_{*m} := \sum_{l=0}^{d-1} A_{lm}$ for one of its marginals. To construct the elements $a_{ij,pq}$, we rewrite (7) as

$$\rho = d^{-1} \sum\nolimits_{lmkk'} A_{lm} z^{l(k-k')}|k, k \ominus m\rangle\langle k', k' \ominus m| \tag{8}$$

and thus find $a_{ij,pq} = d^{-1}\delta_{i\ominus j,p\ominus q} \sum_l A_{l,i\ominus j} z^{l(i-p)}$; since $\delta_{i\ominus j,p\ominus q} = \delta_{i\ominus p,j\ominus q}$, this gives rise to a block structure of the density matrix, where for every $m \in \mathbb{Z}_d$ the basis elements of the

blocks are given by $\{|ip\rangle | i \ominus p = m\}$. Comparing this with the block structure of general $\mathfrak{U}_2$-invariant states, we find the following lemma.

Lemma 3 (Characterization of $\mathfrak{U}_2$-invariant Bell-diagonal states)**.** *A Bell-diagonal state with coefficient system $(A_{lm})_{l,m=0}^{d-1}$ is $\mathfrak{U}_2$-invariant, if and only if for all $m \neq 0$ and $l \in \mathbb{Z}_d$ there holds $A_{lm} = d^{-1} A_{*m}$.*

The two trace conditions of section 2.4 now read

$$\sum_k a_{ijk,pqk} \stackrel{!}{=} a_{ij,pq} = \begin{cases} d^{-1}\tilde{A}_{ip} := d^{-1}\sum_l A_{l0} z^{l(i-p)}, & \text{if} \quad i = j \quad \text{and} \quad p = q \\ d^{-1} A_{*,i\ominus j} = \lambda_{ij}, & \text{if} \quad i = p \quad \text{and} \quad j = q. \end{cases} \tag{9}$$

Note that there is no ambiguity in the case $i = j = p = q$, and the remaining cases are all zero and irrelevant. As in subsection 2.4, the relevant components for the first trace condition lie in the blocks B_k, whilst the relevant components for the second trace condition are precisely the diagonal elements of all blocks.

3.1. Symmetric extensions of $\mathfrak{U}_2$-invariant Bell-diagonal states

The Bell-diagonal states have particular properties, which we can use in our discussion. Namely, the matrix $\tilde{B} = d^{-1}(\tilde{A}_{ip})_{i,p=0}^{d-1}$ of theorem 1 is circulant and the conditions on the diagonal elements of B_k also have the circulant structure $\lambda_{iik} \leqslant d^{-1} A_{*,i\ominus k}$. This will yield some simplifications.

The symmetric group S_d can be seen to consist of the permutations on $\mathbb{Z}_d$. Using a permutation $\pi \in S_d$, one can shift rows and columns of a matrix $A = (a_{ij})_{i,j=0}^{d-1} \in \mathbb{C}^{d\times d}$ to get $A^{(\pi)} = (a_{\pi(i),\pi(j)})_{i,j=0}^{d-1}$. (Technically spoken, this is a representation of S_d on $\mathbb{C}^{d\times d}$.) For the cyclic permutation defined by $\pi_l(i) := i \ominus l$, we shall write $A^{(l)} := A^{(\pi_l)}$. With this definition we can simplify theorem 1 in the case of Bell-diagonal states.

Theorem 2 (Symmetric extendibility of $\mathfrak{U}_2$-invariant Bell-diagonal states)**.** *For a $\mathfrak{U}_2$-invariant Bell-diagonal symmetrically extendible state, the set of matrices in theorem 1 can be chosen to consist of matrices $B_0, B_1, \ldots, B_{d-1}$, such that $B_l = B_0^{(l)}$ holds for all $l \in \mathbb{Z}_d$.*

Proof. First note that in the Bell-diagonal case, the matrix $\tilde{B}$ of theorem 1 is circulant in the Bell-diagonal case, i.e. $\tilde{B} = \tilde{B}^{(l)}$ for all $l \in \mathbb{Z}_d$. This implies

$$\tilde{B} = \tilde{B}^{(l)} = B_0^{(l)} + B_1^{(l)} + B_2^{(l)} + \cdots + B_{d-1}^{(l)}, \tag{10}$$

and we can define $B'_k := d^{-1}\sum_{l=0}^{d-1} B_{k\ominus l}^{(l)}$ for all $k \in \mathbb{Z}_d$. Since the matrix $B_k^{(l)}$ fulfils the same diagonal constraints as $B_{k\oplus l}$, the matrix B'_k fulfils the same conditions as B_k, and $\sum_{k=0}^{d-1} B'_k = \tilde{B}$. □

This theorem tells us that we effectively have to look for *one* matrix B_0 only instead of d matrices. Corollary 1 now states that symmetrically extendible $\mathfrak{U}_2$-invariant Bell-diagonal states fulfil $|\tilde{A}_{ip}| \leqslant \sum_{k=0}^{d-1} \sqrt{A_{*k} A_{*,k\oplus i\ominus p}}$ for all $i, p \in \mathbb{Z}_d$.

3.2. Generalized-isotropic states

We now want to concentrate on an even more restricted class of states, where we can solve the problem completely, the *generalized isotropic states* [3]. These are Bell-diagonal states where $A_{l0} = A_{l'0}$, $A_{0m} = A_{0m'}$ and $A_{lm} = A_{l'm'}$ hold for all $l, m \neq 0$. Since we enforce

$\mathfrak{U}_2$-invariance and normalization, we are left with two parameters, a and b only, for which there hold $a, b \geqslant 0$ and $x := a + (d-1)b \leqslant 1$; we have

$$A_{lm} = \begin{cases} a, & \text{if} \quad l = m = 0, \\ b, & \text{if} \quad l \neq m = 0, \\ \frac{1-a-(d-1)b}{d(d-1)} & \text{else.} \end{cases} \tag{11}$$

In particular, $A_{*m} = \delta_{m0} \cdot x + (1-\delta_{m0}) \cdot \frac{1-x}{d-1}$ and $\sum_l A_{l0} z^{l(i-p)} = \delta_{ip} \cdot x + (1-\delta_{ip})(a-b)$. Considering the matrix B_0' of theorem 2, the constraints on the diagonal elements read $a_{000,000} \leqslant d^{-1} \cdot x$ and $a_{ii0,ii0} \leqslant d^{-1} \cdot \frac{1-x}{d-1}$ for $i \neq 0$. We shall now consider the matrix B_0'', where we average all rows and columns except the first one:

$$B_0'' := \frac{1}{(d-1)!} \sum\nolimits_{\pi \in \{\varphi \in S_d | \varphi(0)=0\}} B_0'^{(\pi)}. \tag{12}$$

A positive sum of positive matrices being positive, the matrix B_0'' is positive and can replace B_0' in theorem 2, because the sums of the off-diagonal components are the same as in B_0', as is shown in the following. The use of this mixing over several permutations enforces some symmetries; we write $B_0' = (b_{ij})_{i,j=0}^{d-1}$ for $b_{ij} := a_{ii0,jj0}$:

(i) the entry b_{00} remains unaffected and invariant;
(ii) the entries b_{0j}, $j \neq 0$, are mapped to $(d-1)^{-1}(b_{01} + b_{02} + \cdots + b_{0,d-1})$;
(iii) the entries b_{i0}, $i \neq 0$, are mapped to $(d-1)^{-1}(b_{10} + b_{20} + \cdots + b_{d-1,0})$;
(iv) the entries b_{ij}, $i = j \neq 0$, are mapped to $(d-1)^{-1}(b_{11} + b_{22} + \cdots + b_{d-1,d-1})$;
(v) the entries b_{ij}, $i \neq j, i, j \neq 0$, are mapped to $(d-1)^{-1}(d-2)^{-1} \sum_{i \neq j, i, j \neq 0} b_{ij}$.

We can thus focus on matrices of the form $B_0'' = d^{-1} M_d(\alpha, \beta, \xi, \eta)$, where

$$M_d(\alpha, \beta, \xi, \eta) := \begin{pmatrix} \alpha & \xi^* & \xi^* & \dots & \xi^* \\ \xi & \beta & \eta & \dots & \eta \\ \xi & \eta & \beta & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \eta \\ \xi & \eta & \dots & \eta & \beta \end{pmatrix} \in \mathbb{C}^{d \times d}; \tag{13}$$

the determinant of this matrix is given by

$$\det M_d(\alpha, \beta, \xi, \eta) = (\beta - \eta)^{d-2} \{\alpha[\beta + (d-2)\eta] - (d-1)|\xi|^2\}. \tag{14}$$

In order for B_0'' to be Hermitian, α, β and η must be real; the parameter ξ can be chosen to be real, since $\xi + \xi^* + (d-2)\eta \stackrel{!}{=} a - b$ is real, and replacing ξ by its real part $\operatorname{Re} \xi$ does not change the sum and does not harm positivity of the matrix, which is a consequence of the following lemma.

Lemma 4 (Positive semidefinite matrices)**.** *The matrix $M_d(\alpha, \beta, \xi, \eta)$ is positive semidefinite, if and only if the three quantities α, β and $\det M_d(\alpha, \beta, \xi, \eta)$ are jointly non-negative, the inequality $|\xi| \leqslant \sqrt{\alpha\beta}$ holds and $\eta \in \left[-\frac{\beta}{d-2}; \beta\right]$.*

Proof. Using lemma 1, we have to check whether all principal minors of $M_d(\alpha, \beta, \xi, \eta)$ are non-negative. The principal minors of order one are α, β, the others can easily seen to be

$$\begin{aligned} &\det M_r(\alpha, \beta, \xi, \eta) \quad \text{for} \quad r \in \{2, \dots, d\}, \\ &\det M_s(\beta, \beta, \eta, \eta) \quad \text{for} \quad s \in \{2, \dots, d-1\}. \end{aligned} \tag{15}$$

By invoking (14) we find $\det M_s(\beta, \beta, \eta, \eta) = (\beta - \eta)^{s-1}[\beta + (s-1)\eta]$, which leads to $\eta \in \left[-\frac{\beta}{d-2}; \beta\right]$. For $\det M_r(\alpha, \beta, \xi, \eta)$ we thus focus on the curly bracket of (14) to find

$(\beta-\eta)^{-(r-1)}\det M_{r+1}(\alpha,\beta,\xi,\eta) = (\beta-\eta)^{-(r-2)}\det M_r(\alpha,\beta,\xi,\eta) + (\alpha\eta - |\xi|^2)$. Since $(\alpha\eta - |\xi|^2)$ is fixed, we only need to consider the cases $r \in \{2, d\}$, which are given by $|\xi| \leqslant \sqrt{\alpha\beta}$ and $\det M_d(\alpha,\beta,\xi,\eta) \geqslant 0$, respectively. □

Let us for now denote by $\rho(a,b)$ the state described by (11), which is the general form of a $\mathfrak{U}_2$-invariant Bell-diagonal generalized-isotropic state. To satisfy theorem 2, $\alpha+(d-1)\beta = a+(d-1)b = x$ must hold. For x being fixed, we may thus write $\alpha = (1-\sigma)x$ and $\beta = \frac{\sigma x}{d-1}$, where the diagonal constraints from theorem 1 read $\sigma \in \left[0; \min\left\{1, \frac{1-x}{x}\right\}\right]$. The following lemma allows us to focus on the extremal values $(a-b)_{\min} \leqslant 0 \leqslant (a-b)_{\max}$ for which the state is symmetrically extendible, given that x is fixed.

Lemma 5 (Mixtures of states)**.** *Given two symmetrically extendible states $\rho(a_1,b_1)$ and $\rho(a_2,b_2)$, such that there holds $x = a_1+(d-1)b_1 = a_2+(d-1)b_2$, any other state $\rho(a,b)$ with $a+(d-1)b = x$ and $a_1-b_1 \leqslant a-b \leqslant a_2-b_2$ is symmetrically extendible.*

Proof. We find $\rho(a,b) = p\cdot\rho(a_1,b_1) + (1-p)\cdot\rho(a_2,b_2)$ for $p := \frac{(a-b)-(a_2-b_2)}{(a_1-b_1)-(a_2-b_2)}$ and note that the set of symmetrically extendible states is convex. □

We will now investigate the possible choices of ξ and η to find the allowed values for $2\xi+(d-2)\eta = a-b$ in the case of $d \geqslant 3$ and comment on $d = 2$ in the following subsection.

3.2.1. Calculation of $(a-b)_{\max}$. To find $(a-b)_{\max}$, it is sufficient to maximize ξ and η individually. We can therefore set $\eta_{\max} := \beta = \frac{\sigma x}{d-1}$, which leads to the maximum range for ξ. The determinant condition $\det M_d(\alpha,\beta,\xi,\eta) \geqslant 0$ leads to

$$|\xi| \leqslant \sqrt{\frac{\alpha[\beta+(d-2)\eta_{\max}]}{d-1}} = \sqrt{\frac{(1-\sigma)x\left[\frac{\sigma x}{d-1}+(d-2)\frac{\sigma x}{d-1}\right]}{d-1}} = x\sqrt{\frac{\sigma(1-\sigma)}{d-1}}, \tag{16}$$

which is precisely the same as $|\xi| \leqslant \sqrt{\alpha\beta}$. We have thus found $\xi_{\max} = x\sqrt{\frac{\sigma(1-\sigma)}{d-1}}$, which results in $(a-b)_{\max} = 2\xi_{\max}+(d-2)\eta_{\max} = x\cdot f(\sigma)$ for

$$f(\sigma) := 2\cdot\sqrt{\frac{\sigma(1-\sigma)}{d-1}} + (d-2)\cdot\frac{\sigma}{d-1}, \tag{17}$$

and we still have to maximize over $\sigma \in \left[0; \min\left\{1, \frac{1-x}{x}\right\}\right]$. The function f monotonically increases up to a maximum value of $f\left(\frac{d-1}{d}\right) = 1$. If the choice of $\sigma := \frac{d-1}{d}$ is allowed, any state with positive $(a-b)$ is symmetrically extendible, since $a-b \leqslant x$ is always true; this holds, if $\frac{d-1}{d} \leqslant \frac{1-x}{x}$ or $x \leqslant \frac{d}{2d-1}$. Else we choose the maximally possible value $\sigma := \frac{1-x}{x}$ to find

$$a-b \leqslant f\left(\frac{1-x}{x}\right)\cdot x = 2\sqrt{\frac{(1-x)(2x-1)}{d-1}} + \frac{d-2}{d-1}\cdot(1-x) \tag{18}$$

as a criterion for symmetric extendibility, given that $a-b \geqslant 0$.

3.2.2. Calculation of $(a-b)_{\min}$. The calculation of $(a-b)_{\min}$ is more involved than the previous one, because we cannot separately minimize ξ and η. We write $\eta = \tau x$ and start with the conditions on ξ:

$$|\xi| \leqslant \sqrt{\frac{\alpha[\beta+(d-2)\eta]}{d-1}} = x\sqrt{\frac{(1-\sigma)\left[\frac{\sigma}{d-1}+(d-2)\tau\right]}{d-1}}. \tag{19}$$

Since $\eta \in \left[\frac{-\beta}{d-2}; \beta\right]$, there must hold $\tau \in \left[\frac{-\sigma}{(d-2)(d-1)}; \frac{\sigma}{d-1}\right]$. We can continue to substitute $\mu := (d-2)(d-1)\tau$ and $\nu := \mu + \sigma$ to find

$$|\xi| \leqslant \frac{x}{d-1}\sqrt{(1-\sigma)(\sigma+\mu)} = \frac{x}{d-1}\sqrt{(1-\sigma)\nu} \tag{20}$$

for $\mu \in [-\sigma; (d-2)\sigma]$ and $\nu \in [0; (d-1)\sigma]$. We can set $\xi_{\min} := -\frac{x}{d-1}\sqrt{(1-\sigma)\nu}$ and minimize the value of

$$2\xi + (d-2)\eta = \frac{x}{d-1} \cdot [-2\sqrt{(1-\sigma)\nu} + (\nu - \sigma)]. \tag{21}$$

The first derivative of the bracket with respect to ν is $1 - \sqrt{\nu^{-1}(1-\sigma)}$, unless $\sigma = 1$ or $\nu = 0$, and the minimum always lies in $[0; (d-1)\sigma]$. The minimum attained is -1, so $(a-b)_{\min} = -\frac{x}{d-1}$, and since smaller values of $(a-b)$ are impossible by definition, *all* states with $a < b$ can be symmetrically extended.

3.3. Discussion of results

Altogether, the last two calculations of $(a-b)_{\max}$ and $(a-b)_{\min}$ have shown the following.

Theorem 3 (Symmetric extendibility of generalized-isotropic states)**.** *For $d \geqslant 3$, a $\mathfrak{U}_2$-invariant Bell-diagonal generalized-isotropic state is symmetrically extendible, if and only if either $x \leqslant \frac{d}{2d-1}$ or inequality (18) or both hold.*

We shall finally discuss the qubit case $d = 2$. The calculations from section 3.2.1 essentially go through, but those of section 3.2.2 fail due to denominators $d-2$. However, by a local unitary operation we can interchange a and b and find that a state with $x \in [1/3; 2/3]$ or

$$|a-b| \leqslant 2\sqrt{(1-x)(2x-1)} \tag{22}$$

is symmetrically extendible; rewriting this yields $-9a^2 - 14ab - 9b^2 + 12a + 12b - 4 \geqslant 0$, which coincides with the results known before [1].

Another important case for two-qudit states are isotropic states (cf section 2). It can be shown that the isotropic states are those Bell-diagonal states where the equality $A_{lm} = \frac{1-A_{00}}{d^2-1}$ holds for all $(l,m) \neq (0,0)$. In this case only a single parameter is left (any one of a, b or x). We find $(a-b)_{\text{isotropic}} = \frac{dx-1}{d-1} > 0$ and by solving (18) we find $x \leqslant \frac{d+3}{2(d+1)}$ or $a = x - (d-1)\frac{1-x}{d(d-1)} \leqslant \frac{d+1}{2d}$ to be necessary and sufficient for symmetric extendibility, if $d \geqslant 3$; for $d = 2$, the condition is $a \in [1/4; 3/4]$.

4. Conclusions

We have derived a criterion for symmetric extendibility of $\mathfrak{U}_2$-invariant two-qudit states in terms of a matrix decomposition (theorem 1). We have simplified this in the case of Bell-diagonal states (theorem 2), and for the two-parameter family of generalized-isotropic $\mathfrak{U}_2$-invariant states, we have completely solved the problem (theorem 3).

In the introduction, we already mentioned that in quantum-cryptographic protocols symmetrically extendible states cannot be used, if only one-way communication between the two parties is allowed. Given symmetrically extendible states, it is therefore necessary to decide whether they can be transformed into non-extendible states by some class of two-way protocols. If this is not the case, no secure key can be distilled by such protocol. From this consideration it is possible to derive upper bounds for quantum-cryptographic protocols using our criteria, and it appears that the already known bounds for two-way quantum cryptography

(e.g. [3, 4]) cannot be increased by standard means of two-way protocols. This extends some of the known results [1, 2] for qubit-based protocols; for details of this extension we refer to [8, 9].

Acknowledgments

The author thanks Gernot Alber, Matthias Christandl, Norbert Lütkenhaus, Geir Ove Myhr and Joseph M Renes for helpful discussions. He was supported by a *Promotionsstipendium* of the TU Darmstadt; financial support by CASED is acknowledged.

References

[1] Myhr G O, Renes J M, Doherty A C and Lütkenhaus N 2009 *Phys. Rev.* A **79** 042329
[2] Myhr G O and Lütkenhaus N 2009 *Phys. Rev.* A **79** 062307
[3] Ranade K S and Alber G 2007 *J. Phys. A: Math. Theor.* **40** 139–53
[4] Chau H F 2005 *IEEE Trans. Inf. Theory* **51** 1451–68
[5] Gottesman D and Lo H-K 2003 *IEEE Trans. Inf. Theory* **49** 457–75
[6] Terhal B M, Doherty A C and Schwab D 2003 *Phys. Rev. Lett.* **90** 157903
[7] Gantmacher F R 1958 *Matrizenrechnung Teil I,* (Berlin: VEB Deutscher Verlag der Wissenschaften)
[8] Ranade K S 2009 *Phys. Rev.* A **80** 022301
[9] Ranade K S 2009 Quantenkryptographie in endlichdimensionalen Systemen *PhD Thesis* http://tuprints.ulb.tu-darmstadt.de/1318/1/Dissertation_160_2009-02-20_modif2.pdf