Asymptotic correctability of Bell-diagonal qudit states and lower bounds on tolerable error probabilities in quantum cryptography

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **40** (2007) 139–153 doi:10.1088/1751-8113/40/1/008

Asymptotic correctability of Bell-diagonal qudit states and lower bounds on tolerable error probabilities in quantum cryptography

Kedar S Ranade and Gernot Alber

Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Deutschland (Germany)

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

Received 26 September 2006, in final form 10 November 2006
Published 6 December 2006
Online at stacks.iop.org/JPhysA/40/139

Abstract

The concept of asymptotic correctability of Bell-diagonal quantum states is generalized to elementary quantum systems of higher dimensions. Based on these results basic properties of quantum state purification protocols are investigated which are capable of purifying tensor products of Bell-diagonal states and which are based on B-steps of the Gottesman-Lo-type with the subsequent application of a Calderbank–Shor–Steane quantum code. Consequences for maximum tolerable error rates of quantum cryptographic protocols are discussed.

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

1. Introduction

Quantum-state purification protocols which are based on local operations and classical communication and which are capable of purifying tensor products of Bell-diagonal quantum states are of considerable current interest in the area of quantum cryptography. This may be traced back to the fact that the security analysis and questions concerning achievable secret-key rates of many quantum cryptographic protocols are based on basic properties of such quantum-state purification protocols [1, 2]. So far, a satisfactory understanding of such protocols has already been obtained in qubit-based scenarios. In particular, it was demonstrated that powerful quantum-state purification protocols can be developed for tensor products of Bell-diagonal states by combining a sufficiently large number of purification steps involving classical two-way communication, so-called B-steps [2], with subsequent quantum error correction based on Calderbank–Shor–Steane (CSS) codes [3] which involve classical one-way communication only. Furthermore, the asymptotic properties of these protocols for large numbers of B-steps can be analysed in a convenient way by characteristic exponents

which govern the relation between bit- and phase errors [4]. Based on such an analysis it is straightforward, for example, to determine maximally tolerable bit-error probabilities of quantum cryptographic protocols of the prepare-and-measure type whose security analysis can be reduced to the purification of Bell-diagonal qubit states [2, 4–6]. Contrary to qubit-based scenarios, elementary properties of quantum-state purification protocols are still rather unexplored in quantum cryptographic contexts in which the transfer of quantum information is based on higher-dimensional elementary quantum systems, so-called qudits.

Recently, some qudit-based quantum cryptographic protocols were developed whose security analysis can be related to basic properties of quantum-state purification protocols capable of purifying tensor products of generalized Bell-diagonal quantum states [7–9]. Motivated by these current developments in this paper the asymptotic properties of qudit-based quantum-state purification protocols are investigated which involve B-steps and the subsequent application of a CSS code fulfilling the Shannon bound of Hamada [10]. For this purpose, the previously developed concept of asymptotic correctability is generalized to arbitrary-dimensional elementary quantum systems and corresponding relevant exponents are determined which govern the relation between dit-and phase errors for large numbers of purification steps (compare with theorem 2). In quantum cryptographic applications, the phase-error probabilities are not accessible to direct measurement, but they have to be estimated on the basis of the measured qudit-error probabilities. For this purpose it is convenient to start a purification protocol with a local unitary mixing transformation which homogenizes the phase errors associated with each possible dit error. The asymptotic correctability under the resulting quantum-state purification protocol can be determined in a rather straightforward way (compare with theorem 4). This latter result is particularly useful for determining lower bounds on maximally tolerable qudit-error probabilities of quantum cryptographic protocols whose security analysis can be reduced to the asymptotic correctability under these latter quantum-state purification protocols.

This paper is organized as follows: in section 2 basic notions of qudit-systems, such as the definition of generalized Bell states, are summarized. Section 3 is devoted to the definition of asymptotic correctability of general quantum state purification protocols which involve tensor products of generalized Bell-diagonal qudit states. In particular, theorem 2 relates this asymptotic correctability to basic properties of exponents which govern the relation between dit and phase errors. Section 4 specializes these results to purification protocols which start with a local mixing operation followed by generalized B-steps and a subsequent application of a CSS quantum code. In section 5 lower bounds on maximally tolerable dit-error probabilities of quantum cryptographic protocols are discussed whose postprocessing can be reduced to the analysis of such purification protocols.

2. Quantum systems of dimension d

We consider a quantum system of dimension d, which is called a qudit. A certain orthonormal basis of the associated Hilbert space $\mathcal{H} = \mathbb{C}^d$ is labelled by the elements of the set $\mathbb{Z}_d := \{0, \ldots, d-1\}$, which are representatives of the ring of residue classes $\mathbb{Z}/\mathrm{d}\mathbb{Z}$, i.e. we consider all operations modulo d; we denote addition and subtraction by '$\oplus$' and '$\ominus$', respectively. We further denote $\mathbb{Z}_d^* := \mathbb{Z}_d \setminus \{0\}$.[1] In analogy with the abbreviation 'bit' for 'binary digit' we use the term 'dit' for 'd-ary digit'.

We will need the notion of a probability distribution on d elements, which can be identified with normalized d-tuples of non-negative real numbers. For convenience, we denote the set

[1] Unless d is a prime, $\mathbb{Z}_d^*$ does not represent the set of invertible elements of $\mathbb{Z}/\mathrm{d}\mathbb{Z}$.

of such tuples by

$$\mathcal{W}_d := \left\{ (p_0, \ldots, p_{d-1}) \in \mathbb{R}^d \,\middle|\, \sum_{i=0}^{d-1} p_i = 1;\ p_i \geqslant 0 \quad \text{for all } i \right\}. \tag{1}$$

For such a probability distribution $p = (p_0, \ldots, p_{d-1}) \in \mathcal{W}_d$ the Shannon entropy is defined by

$$H_d(p) := -\sum_{i=0}^{d-1} p_i \log_d p_i = -(\ln d)^{-1} \sum_{i=0}^{d-1} p_i \ln p_i. \tag{2}$$

The Hilbert space of a pair of qudits, i.e. $\mathcal{H} \otimes \mathcal{H}$, has a basis of maximally entangled states, which we call the *(generalized) Bell basis* of this system. It is defined by [11]

$$|\Psi_{lm}\rangle := \frac{1}{\sqrt{d}} \left[\sum_{k=0}^{d-1} z^{lk} |k\rangle |k \ominus m\rangle \right] \qquad \text{for} \quad l, m \in \mathbb{Z}_d, \tag{3}$$

where $z := \exp(2\pi \mathrm{i}/d)$ is the principal root of unity of order d. We denote the associated density matrices by $(l, m) := |\Psi_{lm}\rangle\langle\Psi_{lm}|$. We will frequently use classical mixtures of generalized Bell states, i.e. states of the form

$$\rho = \sum_{l,m=0}^{d-1} A_{lm} |\Psi_{lm}\rangle\langle\Psi_{lm}|, \qquad \text{where} \quad (A_{lm})_{l,m=0}^{d-1} \in \mathcal{W}_{d\times d}. \tag{4}$$

Such mixtures we will identify with their coefficient matrix[2], so that we can write

$$\rho = (A_{lm})_{l,m=0}^{d-1} = \begin{pmatrix} A_{00} & A_{01} & \ldots & A_{0,d-1} \\ A_{10} & A_{11} & \ldots & A_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{d-1,0} & A_{d-1,1} & \ldots & A_{d-1,d-1} \end{pmatrix}. \tag{5}$$

The only condition on the entries is that they form a probability distribution on $\mathbb{Z}_d \times \mathbb{Z}_d$, i.e. that all A_{lm} are non-negative and sum up to one. The set of all such mixtures of generalized Bell states will be denoted by $\mathcal{S}_{\mathrm{bd}}^{(d)}$.

We will consider $|\Psi_{00}\rangle$ as the reference state for purification, so that we can interpret l and m as phase and dit errors, respectively. The columns of the coefficient matrix thus represent different dit values, whereas the rows represent different phase values. Marginal distributions of dit and phase errors are therefore given by

$$A_{*m} := \sum_{l=0}^{d-1} A_{lm} \quad \text{for} \quad m \in \mathbb{Z}_d \qquad \text{and} \qquad A_{l*} := \sum_{m=0}^{d-1} A_{lm} \quad \text{for} \quad l \in \mathbb{Z}_d. \tag{6}$$

A generalized XOR operation on two qudits, the control and the target, is defined by $\mathrm{GXOR}|k\rangle|l\rangle := |k\rangle|k \ominus l\rangle$ [11]. The bilateral version applied to two pure generalized Bell states (l_1, m_1) and (l_2, m_2) yields

$$\mathrm{GBXOR}[(l_1, m_1) \otimes (l_2, m_2)] = (l_1 \oplus l_2, m_1) \otimes (l_2, m_1 \ominus m_2). \tag{7}$$

Another mathematical tool which we use is the so-called p-norm for tuples of fixed length, where $p \in [1; \infty]$. For $x = (x_0, x_1, \ldots, x_{d-1}) \in \mathbb{C}^d$ it is defined by

$$\|x\|_p := \left(\sum_{i=0}^{d-1} |x_i|^p \right)^{1/p} \tag{8}$$

[2] The coefficient matrix is not a density matrix on a Hilbert space.

for $p \in [1;\infty)$ and $\|x\|_\infty := \max\{|x_i||i \in \mathbb{Z}_d\}$. We have $\|x\|_p \geqslant \|x\|_q$ for $p \leqslant q$ and $\lim_{p\to\infty}\|x\|_p = \|x\|_\infty$. If $|x_i| \leqslant 1$ for all i (which e.g. is the case, if $x \in \mathcal{W}_d$), also $\|x\|_p^p \geqslant \|x\|_q^q$ holds. Of particular interest is the fact that the 2-norm is invariant with respect to a discrete Fourier transform.

3. Asymptotic correctability for qudit systems

In this section, we consider entanglement purification protocols and their properties. We assume that two distant parties, Alice and Bob, share a large amount of mixtures of generalized Bell states, i.e. their joint state is $\rho^{\otimes n}$ for $\rho \in \mathcal{S}_{\mathrm{bd}}^{(d)}$ and some large $n \in \mathbb{N}$. They perform two-way entanglement purification until the use of a CSS code fulfilling the quantum Shannon bound allows them to extract some pure generalized Bell state, e.g. $|\Psi_{00}\rangle$. The quantum Shannon bound is given by the following theorem.

Theorem 1 (quantum Shannon bound)**.** *Let d be a prime number and consider a state $\rho = (A_{lm})_{l,m=0}^{d-1} \in \mathcal{S}_{\mathrm{bd}}^{(d)}$. If*

$$\mathrm{AsymCSS}\left[(A_{lm})_{l,m=0}^{d-1}\right] := 1 - H_d\left[(A_{*m})_{m=0}^{d-1}\right] - H_d\left[(A_{l*})_{l=0}^{d-1}\right] > 0,$$

there exists a CSS code which can correct a tensor product state $\rho^{\otimes n}$.

Proof. This is an obvious consequence of a theorem by Hamada ([10], theorem 2). □

Using this bound, we can now define the notion of asymptotic correctability; due to the use of that theorem, in the following we consider d always to be prime. For $d = 2$, this definition reduces to that given in [4].

A correction step $S_n^{(d)}$ of a quantum state purification protocol takes as input a state of the form $\rho^{\otimes n}$ and outputs a state of the form $\rho'^{\otimes n'}$, where $\rho, \rho' \in \mathcal{S}_{\mathrm{bd}}^{(d)}$. In general, $n' \leqslant n$ and ρ' is supposed to be more entangled than ρ. Occasionally, a step may fail and does not output anything. As we do not consider distillation rates we can drop the labels n and n'. A correction step will thus be treated as a function on $\mathcal{S}_{\mathrm{bd}}^{(d)}$, mapping $(A_{lm})_{l,m=0}^{d-1}$ to $(A'_{lm})_{l,m=0}^{d-1}$.

Definition 1 (asymptotic correctability)**.** *Let $\rho = (A_{lm})_{l,m=0}^{d-1} \in \mathcal{S}_{\mathrm{bd}}^{(d)}$ and $\left(S_n^{(d)}\right)_{n\in\mathbb{N}}$ be a sequence of possible correction steps in an entanglement purification protocol. The state ρ is called asymptotically $S_n^{(d)}$-correctable, if the inequality $\mathrm{AsymCSS}\left[S_n^{(d)}(\rho)\right] > 0$ holds for all $n \geqslant N_0$, where $N_0 \in \mathbb{N}$. We call ρ asymptotically non-correctable under the sequence $\left(S_n^{(d)}\right)_{n\in\mathbb{N}}$, if $\mathrm{AsymCSS}\left[S_n^{(d)}(\rho)\right] \leqslant 0$ holds for $n \geqslant N_0$ for some $N_0 \in \mathbb{N}$.*

We now want to generalize the criterion for asymptotic correctability of [4] to qudits. It turns out that this generalization is straightforward and essentially is a reformulation of the previous result. The main difficulty in the proof lies in dealing with Shannon entropies for d elements instead of the binary Shannon entropy.

As in the qubit case we focus on Taylor expansions of the Shannon entropy. The following two lemmata will considerably simplify our approach.

Lemma 1 (bounds for the Shannon entropy)**.** *Let $\xi = (\xi_0, \ldots, \xi_{d-1}) \in \mathcal{W}_d$ and set $x_n := \sum_{i=1}^{d-1}\xi_i = 1 - \xi_0$. If we associate with ξ the distributions $\xi_{\min} := (\xi_0, x_n, 0, \ldots, 0)$ and $\xi_{\max} := \left(\xi_0, \frac{x_n}{d-1}, \ldots, \frac{x_n}{d-1}\right)$, then*

$$H_d(\xi_{\min}) \leqslant H_d(\xi) \leqslant H_d(\xi_{\max})$$

holds, and we calculate

$$H_d(\xi_{\min}) = -(\ln d)^{-1}[\xi_0 \ln \xi_0 + x_n \ln x_n],$$
$$H_d(\xi_{\max}) = -(\ln d)^{-1}\left[\xi_0 \ln \xi_0 + x_n \ln \frac{x_n}{d-1}\right].$$

Proof. See appendix A. □

Lemma 2 (a Taylor expansion for the Shannon entropy)**.** *Let $p = (p_0, \ldots, p_{d-1}) \in \mathcal{W}_d$ and denote by $g := (1/d, \ldots, 1/d) \in \mathcal{W}_d$ the uniform probability distribution on a set with d elements. Provided that there exists some factor $f > 0$, such that $p_i \geqslant f/d$ holds for all i, we have*

$$H_d(p) = 1 - K\|g - p\|_2^2 + K'\varepsilon(p)\|g - p\|_3^3$$

for some $K, K' > 0$ and a bounded function $\varepsilon : \mathcal{W}_d \to [-1; 1]$.

Proof. See appendix B. □

The following theorem now generalizes theorem 1 of [4] to higher dimensions.

Theorem 2 (asymptotic correctability)**.** *Let d be prime and $\rho = (A_{lm})_{l,m=0}^{d-1} \in \mathcal{S}_{\text{bd}}^{(d)}$ be a state on which for each $n \in \mathbb{N}$ a (fictive) $S_n^{(d)}$ step is applied to; the resulting state shall be called $(A'_{lm})_{l,m=0}^{d-1} \in \mathcal{S}_{\text{bd}}^{(d)}$. Define by*

- $x_n := \sum_{m=1}^{d-1} \sum_{l=0}^{d-1} A'_{lm}$ *the total dit-error rate;*
- $y_n := \|g - p\|_2/\sqrt{2}$ *a measure for the deviation of the phase error probability $p = (A'_{l*})_{l=0}^{d-1}$ from the uniform probability distribution $g = (1/d, \ldots, 1/d)$.*[3]

Provided that the sequence $(x_n)_{n\in\mathbb{N}}$ converges to zero, we have the following:

(i) If there exists an $r > 2$ such that $\sup\left\{x_n \big/ y_n^r \middle| n \in \mathbb{N}\right\} < \infty$, then ρ is asymptotically S_n-correctable.

(ii) If, on the other hand, $\inf\left\{x_n \big/ y_n^2 \middle| n \in \mathbb{N}\right\} > 0$ holds, then ρ is asymptotically non-correctable with respect to that sequence.

Both statements remain valid if the role of dit errors and phase errors is interchanged.

Proof. We may assume that $\lim_{n\to\infty} y_n = 0$; otherwise our statement follows directly from theorem 1. Considering the distribution of dit errors $\xi = (A_{*m})_{m=0}^{d-1}$ and using the binary Shannon entropy $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$, lemma 1 allows us to write

$$H_d(\xi) = L \cdot H(x_n) + c(\xi)x_n, \tag{9}$$

where $L = \ln 2/\ln d$ and $c : \mathcal{W}_d \to [0; \log_d(d-1)] \subseteq [0; 1]$ is some bounded function. By lemma 2, for the distribution of phase errors p due to $\left(2y_n^2\right)^{3/2} = \|g - p\|_2^3 \geqslant \|g - p\|_3^3$ we have

$$H_d(p) = 1 - K \cdot 2y_n^2 + K'\varepsilon(p)\|g - p\|_3^3 \tag{10}$$
$$= 1 - K \cdot 2y_n^2 + K'\varepsilon'(p) \cdot \left(2y_n^2\right)^{3/2}, \tag{11}$$

[3] The factor $\sqrt{2}$ next to y_n is only for consistency of notation with the qubit case [4].

where $K, K' > 0$ and $\varepsilon, \varepsilon' : \mathcal{W}_d \to [-1; 1]$ are bounded functions, provided y_n is sufficiently small. Setting $\rho' := (A'_{lm})_{l,m=0}^{d-1}$ yields

$$\text{AsymCSS}(\rho') = 1 - H_d(\xi) - H_d(p) \tag{12}$$

$$= -L \cdot H(x_n) - c(\xi)x_n + 2K \cdot y_n^2 - 2\sqrt{2}K'\varepsilon'(p) \cdot y_n^3, \tag{13}$$

that is

$$\text{AsymCSS}(\rho') > 0 \quad \Leftrightarrow \quad \frac{-L \cdot H(x_n)}{y_n^2} - c(\xi)\frac{x_n}{y_n^2} + 2K - 2\sqrt{2}K'\varepsilon'(p) \cdot y_n > 0. \tag{14}$$

In the following, we will also use the property that $\lim_{x\to 0^+} H(x)/x^s = 0$ for $s \in [0; 1)$ and $\lim_{x\to 0^+} H(x)/x^s = +\infty$ for $s \in [1; \infty)$.

For the proof of statement (i), note that condition (i) now implies that $x_n \leqslant c y_n^r$ for some $c \geqslant 0$, which yields $-L \cdot H(x_n)/y_n^2 \geqslant -L \cdot c^{2/r} H(x_n)/x^{2/r} \to 0$ for $n \to \infty$ due to $r > 2$. This means that in (14) all terms except $2K$ converge to zero. For the proof of (ii), we have $x_n \geqslant c y_n^2$ for some $c > 0$. In a similar fashion as before, this results in $-L \cdot H(x_n)/y_n^2 \leqslant -L \cdot cH(x_n)/x \to -\infty$. Also, the second term is negative, whereas all other terms are bounded, so that for sufficiently large n the quantum Shannon bound is not fulfilled. □

4. Entanglement purification protocols and asymptotic correctability

In this section, we want to apply our criterion to an actual sequence of correction steps. We therefore focus on a well-known example for two-way entanglement purification, which we will call $B_n^{(d)}$ steps and which are defined for any $n \in \mathbb{N}$. Considering a state $\rho = (A_{lm})_{l,m=0}^{d-1} \in \mathcal{S}_{\text{bd}}$, the main objective of this section is to derive a condition on ρ for asymptotic $B_n^{(d)}$-correctability. It will turn out that we can calculate a *characteristic exponent* $r^{(d)}$, such that for the case $r^{(d)} > 2$ we have asymptotic $B_n^{(d)}$-correctability, whereas for $r^{(d)} \leqslant 2$ we have non-correctability. These results generalize our previous results from [4] from qubits to qudits.

4.1. Bell diagonal states and $B_n^{(d)}$ steps

We now introduce a generalization of the B_n step of [4] to d dimensions. For $n \in \mathbb{N}$, a $B_n^{(d)}$ step is defined by the following procedure.

(i) Alice and Bob arbitrarily choose n qudit pairs $QP_1, \ldots, QP_n$.
(ii) Alice and Bob apply $n - 1$ GBXOR transformations with control QP_1 and target pairs $QP_2, \ldots, QP_n$.
(iii) Alice and Bob measure the dit parity on the pairs $QP_2, \ldots, QP_n$ and discard the measured pairs. They keep QP_1, if and only if all parities are zero, otherwise they discard it.

Starting with a tensor product of Bell states, the transformation of step (ii) is given by

$$\bigotimes_{i=1}^{n} (l_i, m_i) \mapsto \left(\bigoplus_{i=1}^{n} l_i, m_1 \right) \otimes \left[\bigotimes_{k=2}^{n} (l_k, m_1 \ominus m_k) \right]. \tag{15}$$

The first pair is thus kept, if $m_1 \ominus m_k = 0$ holds for all $k \in \{2, \ldots, n\}$.

Because we deal with mixtures of generalized Bell states, we want to formulate a $B_n^{(d)}$ step as a mapping on the set $\mathcal{S}_{\text{bd}}^{(d)}$. This is done in the following theorem.

Theorem 3 (evolution of states for $B_n^{(d)}$ steps)**.** *For each* $k \in \{1, \ldots, n\}$ *let* $\rho^{(k)} = \left(A_{lm}^{(k)}\right)_{l,m=0}^{d-1} \in \mathcal{S}_{\mathrm{bd}}^{(d)}$ *be a state. If a* $B_n^{(d)}$ *step is applied to these states and if not all pairs are discarded, the state of the remaining pair is given by* $\rho' = (A'_{lm})_{l,m=0}^{d-1} \in \mathcal{S}_{\mathrm{bd}}^{(d)}$ *with coefficients*

$$A'_{lm} = (dN)^{-1} \sum_{i=0}^{d-1} \left[z^{-il} \prod_{k=1}^{n} \left(\sum_{j=0}^{d-1} z^{ij} A_{jm}^{(k)} \right) \right],$$

where $z := \exp(2\pi \mathrm{i}/d)$ *denotes the principal value of the root of unity of order* d *and* $N := \sum_{m=0}^{d-1} \left[\prod_{k=1}^{n} \left(\sum_{l=0}^{d-1} A_{lm}^{(k)} \right) \right]$ *is the normalization constant, i.e. the probability of survival of the first qudit pair. Note that the final state is itself Bell diagonal and does not depend on the order of the initial states.*

Proof. See appendix C. □

Although we will not use it, it may be worth mentioning that a sequence of a $B_n^{(d)}$ step and a $B_m^{(d)}$ step is equivalent to a single $B_{n \cdot m}^{(d)}$ step.

4.2. Asymptotic correctability using a sequence of $B_n^{(d)}$ *steps*

Before we proceed with the calculation, we have to introduce some notation. As might be seen from theorem 2, we mainly have to focus on purely exponential behaviour, that is, in many equations we will skip subexponential terms. To be precise, for some non-negative-valued function f, we define its exponent by $z(f) := \lim_{n\to\infty} \sqrt[n]{f(n)}$, where we always assume that this limit exists; any such function may now be written as $f(n) = c(n)z^n$ for some subexponential function c, i.e. some function c such that $z(c) = 1$ holds. We call two-functions f and g *asymptotically exponentially equal*, if $z(f) = z(g)$, in which case we shall write $f \overset{a.e.}{=} g$.

For simplicity we will further assume that $A_{*0} > \max\{A_{*m} | m \in \mathbb{Z}_d^*\}$ holds; if this is not the case, we can apply the local-unitary operation $\mathbb{1} \otimes \sum_{k\in\mathbb{Z}_d} |k \ominus m\rangle\langle k|$, provided that A_{*m} is the unique largest dit-error probability. We further assume that the phase error rates converge to the uniform probability distribution, which is always the case unless the component of the Fourier transform of the first column which has maximum absolute value is not unique.

4.3. Evolution of dit errors

The evolution of dit errors is straightforward. We denote by $\xi = (\xi_0, \ldots, \xi_{d-1}) \in \mathcal{W}_d$ the distribution of dit errors, i.e. $\xi_m := A_{*m}$ for $m \in \mathbb{Z}_d$. The application of a $B_n^{(d)}$ step may be viewed as a mapping $B_n^{(d)} : \xi \mapsto \xi'$, defined by

$$\xi'_i = \frac{\xi_i^n}{\xi_0^n + \cdots + \xi_{d-1}^n} \qquad \text{for} \quad i \in \mathbb{Z}_d, \tag{16}$$

which follows directly from theorem 3. Therefore, using the notation of theorem 2,

$$x_n := 1 - \xi'_0 = \frac{\sum_{m=1}^{d-1} \xi_m^n}{\sum_{m=0}^{d-1} \xi_m^n} = \left[\frac{\sum_{m=0}^{d-1} \xi_m^n}{\sum_{m=1}^{d-1} \xi_m^n} \right]^{-1} = \left[1 + \frac{\xi_0^n}{\sum_{m=1}^{d-1} \xi_m^n} \right]^{-1}. \tag{17}$$

Setting $\xi_{\max} := \max\{\xi_m | m \in \mathbb{Z}_d^*\}$, the following inequality holds for the denominator:

$$\xi_{\max}^n \leqslant \sum_{m=1}^{d-1} \xi_m^n \leqslant (d-1)\xi_{\max}^n. \tag{18}$$

Using an appropriate function $h : \mathcal{W}_d \to [1; d-1]$ yields

$$x_n = \left[1 + \frac{\xi_0^n}{h(\xi)\xi_{\max}^n}\right]^{-1} =: u(n)\tilde{x}^{-n}, \tag{19}$$

where $\tilde{x} := \xi_0/\xi_{\max} > 1$ and appropriate values $u(n) \in [1/2; d]$. In particular, we have $x_n \overset{a.e.}{=} \tilde{x}^{-n}$ and $\lim_{n\to\infty} \xi'_m = \delta_{m,0}$, so that the correction of dit errors is guaranteed under $B_n^{(d)}$ steps.

4.4. The evolution of phase errors

In comparison to the dit-error evolution, the calculation of the phase errors is more sophisticated. For using theorem 2, we only need to calculate the value $2y_n^2 = \|g - p\|_2^2$, where p is the phase error distribution ($p_l := A_{l*}$) and $g = (1/d, \ldots, 1/d)$ is the uniform probability distribution. By use of theorem 3, it follows

$$2y_n^2 = \|g - p\|_2^2 = \left\| \left(\frac{1}{d} - \frac{\sum_m \sum_i z^{-il} \left(\sum_j z^{ij} A_{jm}\right)^n}{dN} \right)_{l=0}^{d-1} \right\|_2^2. \tag{20}$$

The 2-norm is invariant with respect to a discrete Fourier transform $(x_i)_i \mapsto \left(d^{-1/2} \sum_{i=0}^{d-1} z^{ij} x_i\right)_j$. Thus the use of $\sum_{i=0}^{d-1} z^{ik} = d\delta_{k,0}$ implies

$$2y_n^2 = \frac{1}{d} \left\| \left(\delta_{l,0} - \frac{\sum_m \left(\sum_j z^{lj} A_{jm}\right)^n}{N} \right)_{l=0}^{d-1} \right\|_2^2. \tag{21}$$

The zero component cancels against the normalization; this yields

$$2y_n^2 = \frac{1}{d} \left\| \left(\frac{\sum_m \left(\sum_j z^{lj} A_{jm}\right)^n}{N} \right)_{l=1}^{d-1} \right\|_2^2, \tag{22}$$

where we take the 2-norm on $d-1$ elements only. The evaluation in the general case is complicated, although one may expect that in the limit $n \to \infty$ only the first column of $(A_{lm})_{l,m=0}^{d-1}$ should be relevant. In the next section, we will slightly modify the protocol, so that a calculation of the exponential behaviour of $2y_n^2$ for the modified protocol becomes possible.

4.5. The mixing operation

Consider the single-qudit transformation $U_1 := \sum_{x=0}^{d-1} z^{-x^2} |x\rangle\langle x|$ and define

$$U := U_1 \otimes U_1^* = \sum_{x,y=0}^{d-1} z^{y^2 - x^2} |x\rangle\langle x| \otimes |y\rangle\langle y|. \tag{23}$$

This implies $U|\Psi_{lm}\rangle = z^{m^2} |\Psi_{l\ominus 2m,m}\rangle$ or $U : (l, m) \mapsto (l \ominus 2m, m)$. That is, the transformation of a Bell-diagonal state by the local unitary operation U permutes the coefficients within a fixed column of the coefficient matrix. This property can be used to simplify the calculation of $2y_n^2$; we therefore introduce the following step immediately before Alice and Bob apply the $B_n^{(d)}$ step.

- For each qudit pair Alice and Bob randomly choose a value $n \in \mathbb{Z}_d$ and apply U^n to the respective pair.

Considering a density matrix ρ, this means $\rho \mapsto d^{-1}\sum_{n=0}^{d-1} U^n \rho (U^\dagger)^n$. For a mixture of Bell states, $\rho = (A_{lm})_{l,m=0}^{d-1}$, this step mixes the entries in the columns. Complete mixing within column m, i.e. $A_{lm} \mapsto A_{*m}/d$, will take place, if $2m$ and the dimension d are coprime. If we want to have complete mixing for all columns except the $m = 0$ column, we have to restrict our considerations to odd primes (which we already did due to the use of theorem 1); the case $d = 2$ (the only even prime) was done in [4].

For fixed $l \in \mathbb{Z}_d$, one can calculate

$$\sum_{m=0}^{d-1}\left(\sum_{j=0}^{d-1} z^{lj} A_{jm}\right)^n = \left(\sum_{j=0}^{d-1} z^{lj} A_{j0}\right)^n + \sum_{m=1}^{d-1}\left(\sum_{j=0}^{d-1} z^{lj}\frac{A_{*m}}{d}\right)^n \tag{24}$$

$$= \left(\sum_{j=0}^{d-1} z^{lj} A_{j0}\right)^n + \sum_{m=1}^{d-1}\left(\frac{A_{*m}}{d}\right)^n \underbrace{\left(\sum_{j=0}^{d-1} z^{lj}\right)^n}_{=d\cdot\delta_{l,0}} \tag{25}$$

and due to $l \neq 0$ in (22) it follows

$$2y_n^2 \cdot dN^2 = \left\| \left(\left(\sum_{j=0}^{d-1} z^{lj} A_{j0} \right)^n \right)_{l=1}^{d-1} \right\|_2^2 = \left\| \left(\sum_{j=0}^{d-1} z^{lj} A_{j0} \right)_{l=1}^{d-1} \right\|_{2n}^{2n}. \tag{26}$$

It can now be seen that $\|x\|_{2n}^{2n} = K(n)\|x\|_\infty^n$ for any d-tuple x, where $K(n) \in [1; d]$ may depend on x. This yields

$$2y_n^2 \cdot dN^2 = K(n) \left\| \left(\sum_{j=0}^{d-1} z^{lj} A_{j0} \right)_{l=1}^{d-1} \right\|_\infty^{2n} \tag{27}$$

$$= K(n) \left[\max \left| \sum_{j=0}^{d-1} z^{lj} A_{j0} \right| \middle| l \in \mathbb{Z}_d^* \right]^{2n}. \tag{28}$$

This shows that the determination of the evolution of phase errors is related to the search for the largest absolute value of the Fourier transform of a probability distribution, where the zero component of the transformed tuple is ignored.

4.6. Exponential behaviour

Up to now, we have shown $x_n \overset{a.e.}{=} \tilde{x}^{-n}$, where $\tilde{x} = A_{*0}/\max\{A_{*m} | m \in \mathbb{Z}_d^*\}$. This implies for the normalization constant of a $B_n^{(d)}$ step that $N_n = K'(n) A_{*0}^n$ for $K'(n) \in [1; d]$. Thus we find

$$2y_n^2 = \frac{1}{d} \cdot \frac{K(n)}{K'(n)^2} \cdot \left(\frac{\max\left\{ \left| \sum_j z^{lj} A_{j0} \right| \middle| l \in \mathbb{Z}_d^* \right\}}{A_{*0}} \right)^{2n} =: \frac{K(n)}{K'(n)^2} \cdot \frac{\tilde{y}^{2n}}{d}. \tag{29}$$

The condition $x_n \overset{a.e.}{=} y_n^{r^{(d)}}$ now yields $\tilde{x}^{-n} = \tilde{y}^{r^{(d)} n}$ or

$$r^{(d)} = -\frac{\ln \tilde{x}}{\ln \tilde{y}} = \frac{\ln[A_{*0}/\max\{A_{*m} | m \in \mathbb{Z}_d^*\}]}{\ln\left[A_{*0}/\max\left\{ \left| \sum_j z^{lj} A_{j0} \right| \middle| l \in \mathbb{Z}_d^* \right\}\right]}. \tag{30}$$

This generalizes the characteristic exponent r from our previous work [4] from qubits to qudits.

Finally, we have to relate the characteristic exponent $r^{(d)}$ to the conditions in theorem 2; this we will do in the following theorem.

Theorem 4 (asymptotical $B_n^{(d)}$-correctability)**.** *A state $\rho = (A_{lm})_{l,m=0}^{d-1} \in \mathcal{S}_{\mathrm{bd}}^{(d)}$ is asymptotically $B_n^{(d)}$-correctable, if and only if $r^{(d)} > 2$.*

Proof. Setting $r := r^{(d)}$ and using (19) and (29) we find

$$\frac{x_n}{y_n^r} = u(n)\tilde{x}^{-1} \cdot \left(\tilde{y}^{2n}\frac{K(n)}{2dK'(n)}\right)^{-r/2} = \frac{u(n)}{(\tilde{x}\cdot\tilde{y}^r)^n}\left(\frac{K(n)}{2dK'(n)}\right)^{-r/2}. \tag{31}$$

The characteristic exponent $r^{(d)}$ is chosen in such a way that $(\tilde{x}\cdot\tilde{y}^r)^n = 1$ (in particular, $x_n/y_n^r \overset{a.e.}{=} 1$). The remaining terms are bounded for all $n \in \mathbb{N}$ by some lower bound being larger than zero and some upper bound being less than infinity. Thus, theorem 2 implies the assertion. □

5. Applications in quantum cryptography

Let us now consider some cryptographical applications of our theorems. In the generic model of entanglement-based quantum cryptography, Alice prepares the state $|\Psi_{00}\rangle^{\otimes n}$ and sends every second qudit to Bob. The transmission is considered to be insecure, so that Eve can perform general coherent attacks. The task of Alice and Bob is now to estimate the resulting errors and, if possible, to perform entanglement purification. This provides Alice and Bob with (nearly) maximally entangled states, from which they can extract a secret key.

Although in general the total state of Alice and Bob is complicated, a random permutation of their qudit pairs and a fictive-Bell-measurement argument [2] allows us to restrict the theoretical analysis to tensor products of mixtures of generalized Bell states. If we consider protocols consisting of one $B_n^{(d)}$ step for an appropriately chosen $n \in \mathbb{N}$ and the application of a CSS code according to theorem 1, we only have to determine the coefficients $(A_{lm})_{l,m=0}^{d-1}$ in order to determine, whether we can obtain a secret key.

A final remark has to be made on prepare-and-measure protocols. The reduction of CSS-based protocols for qudits was done by Hamada [10] and the reduction of $B_n^{(d)}$ steps also follows the well-known lines (cf e.g. [2, 8]). The only remaining point is the reduction of our mixing operation; but this mixing only mixes phases and does not change any dit value and therefore has no influence on the key. This means Alice and Bob can just skip it in the associated prepare-and-measure protocol.

In the remaining part we will consider states which may appear in a quantum cryptographic protocol, and we will also deal with the problem that in general we cannot infer all coefficients $(A_{lm})_{l,m=0}^{d-1}$ from measurements, but only the dit-error distribution $\xi = (A_{*m})_{m=0}^{d-1}$ can be measured and any further information has to be inferred from symmetries of the protocol.

5.1. The generalized isotropic case

We start with a particularly simple example, namely *generalized isotropic states*, which were also considered in [9]. A generalized isotropic state is of the form

$$\rho = (\alpha,\beta,\gamma,\delta) := \begin{pmatrix} \alpha & \gamma & \cdots & \gamma \\ \beta & \delta & \cdots & \delta \\ \vdots & \vdots & \ddots & \vdots \\ \beta & \delta & \cdots & \delta \end{pmatrix} \in \mathcal{S}_{\mathrm{bd}}^{(d)}. \tag{32}$$

If $\beta = \gamma$, this is called an *isotropic state*. An interesting property of generalized isotropic states is that they remain of this form, if they are subjected to $B_n^{(d)}$ steps; it is thus possible to view a $B_n^{(d)}$ step as a mapping $B_n^{(d)} : (\alpha, \beta, \gamma, \delta) \mapsto (\alpha', \beta', \gamma', \delta')$, where the coefficients are given by

$$\begin{aligned}
\alpha' &= \{[\alpha + (d-1)\beta]^n + (d-1)[\alpha - \beta]^n\}/dN, \\
\beta' &= \{[\alpha + (d-1)\beta]^n - [\alpha - \beta]^n\}/dN, \\
\gamma' &= \{[\gamma + (d-1)\delta]^n + (d-1)[\gamma - \delta]^n\}/dN, \\
\delta' &= \{[\gamma + (d-1)\delta]^n - [\gamma - \delta]^n\}/dN, \\
N &= [\alpha + (d-1)\beta]^n + (d-1)[\gamma + (d-1)\delta]^n.
\end{aligned} \tag{33}$$

Evaluation of (30) now yields

$$r^{(d)} = \left[\ln \frac{\alpha + (d-1)\beta}{\gamma + (d-1)\delta}\right] \Big/ \ln \left[\frac{\alpha + (d-1)\beta}{|\alpha - \beta|}\right], \tag{34}$$

and thus $r^{(d)} > 2 \Leftrightarrow \alpha^2 + (d-1)\beta^2 - [\alpha + (d-1)\beta]/d > 0$. Using $\alpha > \beta$, we regain the result for isotropic channels of our previous work [9]. Further, the protocol of Chau [7] yields isotropic states with $\beta = \gamma = \delta$, so that we can regain the tolerable error rates of his protocol for primes ([7], table 2, first column)[4]. In the case $d = 2$, this state reduces to the general mixture of qubit Bell states as considered in [4]. Further note that in the case of generalized isotropic channels we could have done the calculation for $r^{(d)}$ without the use of the mixing operation.

5.2. *Maximum tolerable error rates for two-basis cryptography*

In quantum cryptography, the protocol in [7] produces isotropic states, where $\beta = \gamma = \delta$, but in general uses a large number of bases. On the other hand, the theoretical analysis of protocols which use only two bases does not, in general, lead to generalized isotropic states.

Let us now focus on protocols which use two Fourier-dual bases and in which the total dit value probabilities A_{*m} ($m \in \mathbb{Z}_d$) are measured. Such protocols were considered in [8] and it was shown there, that for $l, m \in \mathbb{Z}_d$ the symmetry relations

$$A_{lm} = A_{d-m,l} = A_{d-l,d-m} = A_{m,d-l} \tag{35}$$

hold for the quantum states describing Alice's and Bob's entanglement. A consequence of these relations is $A_{l*} = A_{*l}$ for $l \in \mathbb{Z}_d$.

From the measured dit errors A_{*m} a lower bound on $r^{(d)}$ has to be inferred. From (30) it can be seen that we need three quantities to calculate $r^{(d)}$, namely $x := A_{*m}$, $\max\{A_{*m} | m \in \mathbb{Z}_d^*\}$ and

$$M := \max\left\{ \left| \sum_{j=0}^{d-1} z^{lj} A_{j0} \right| \Big| \, l \in \mathbb{Z}_d^* \right\}. \tag{36}$$

We will write $\max\{A_{*m} | m \in \mathbb{Z}_d^*\} = f \cdot (1 - x) \cdot (d-1)^{-1}$, where $f \in [1; d-1]$. The case $f = 1$ is the *apparently isotropic* case, where all A_{*m} for $m \in \mathbb{Z}_d^*$ are equal, whereas $f = d - 1$ relates to those cases, in which there are only errors of one type. Equation (30)

[4] Note that the rates given by our formula also coincide with Chau's rates for prime powers. Although this may not be by accident, this case is not covered by our derivation.

now reads

$$r^{(d)} = \left(\ln \frac{x}{f \cdot \frac{1-x}{d-1}}\right) \cdot \left(\ln \frac{x}{M}\right)^{-1}. \tag{37}$$

The values of x and f can be directly inferred from the measured dit-error probabilities. However, estimating the value of M is more involved. We note that small values of M correspond to small values of $r^{(d)}$. So, for a lower bound on $r^{(d)}$ we need a lower bound on M, which will be derived now.

For any complex number $z \in \mathbb{C}$, we have $|z| \geqslant \mathrm{Re}\, z$ and the maximum over all $l \in \mathbb{Z}_d^*$ is definitely larger than the average over this set. We thus have

$$M \geqslant \max\left\{\mathrm{Re} \sum\nolimits_{j=0}^{d-1} z^{lj} A_{j0} | l \in \mathbb{Z}_d^*\right\} \geqslant \mathrm{Re} \frac{1}{d-1} \sum\nolimits_{l=1}^{d-1} \sum\nolimits_{j=0}^{d-1} z^{lj} A_{j0}. \tag{38}$$

Exchanging the summation and using the fact that $\sum_{l=1}^{d-1} z^{lj} = d\delta_{j,0} - 1$ yields

$$M \geqslant \frac{1}{d-1} \sum\nolimits_{j=0}^{d-1} (d\delta_{j0} - 1) A_{j0} = A_{00} - \frac{\sum_{j=1}^{d-1} A_{j0}}{d-1}. \tag{39}$$

Note that in the case of the generalized isotropic channel this is an equality. Up to this point we have given a simple, but achievable lower bound on M. In order to infer this lower bound from the qudit-error probabilities measurable in the protocol we use the relations

$$A_{*0} = A_{00} + \sum_{l=1}^{d-1} A_{l0} \leqslant A_{00} + \sum_{l=1}^{d-1} A_{l*} = A_{00} + \sum_{l=1}^{d-1} A_{*l} = A_{00} + (1 - A_{*0}), \tag{40}$$

which imply $A_{00} \geqslant 2A_{*0} - 1$. Note that equality holds, if and only if $A_{lm} = 0$ for $(l, m) \in \mathbb{Z}_d^* \times Z_d^*$. Plugging this bound into the bound for M yields

$$M \geqslant x - d \cdot \frac{1-x}{d-1}. \tag{41}$$

The isotropic channel of (32) is the worst case with respect to correctability (i.e., it has the smallest $r^{(d)}$) of all apparently isotropic channels, i.e. channels where $A_{*m} = A_{*m'}$ for all $m, m' \in Z_d^*$. Furthermore, we have equality in (40) and thus in (41), if for this isotropic channel $\delta = 0$ holds; this case was considered in [9]. If we do not have an isotropic channel, the tolerable error rate according to our bound depends on f, which can be seen as a parameter characterizing the non-isotropy of the measured probability distribution.

By plugging in our bound for M and solving for $x = A_{*0}$, we get as a sufficient condition for correctability

$$x > \frac{2d(2d-1) + (d-1)(f + \sqrt{(4d+f)f})}{2[(2d-1)^2 + (d-1)f]}, \tag{42}$$

where we only consider $x > (d+1)/(2d)$ due to the entanglement bound of [8]. In figure 1, we plotted bounds on the maximum tolerable error rate $(1 - x)$ as a function of d. The upper line is the apparently isotropic case ($f = 1$), the lower one the case with just one type of error ($f = d - 1$). The lower bound for the maximum tolerable error rate in a given protocol lies between these two lines. We thus have shown lower bounds on the maximum tolerable

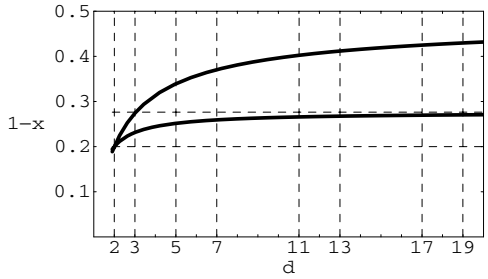

Figure 1. Lower bounds for the maximum tolerable error rate ($1 - x = 1 - A_{*0}$) as a function of the dimension d; the upper line corresponds to the apparently isotropic case $f = 1$ (where this bound is exact), the lower one to the maximum non-isotropy $f = d - 1$. All other cases lie in between. The lines start at $1 - x = 0.2$, the upper one converges to 0.5, the lower one to $1/2 - 1/2\sqrt{5} \approx 0.276$.

error rates of two-basis quantum cryptography using the protocols considered. In the case of apparently isotropic channels our bounds are the best possible lower bounds, in other cases they become worse the more non-isotropic the channel gets.

6. Conclusions

We have generalized the ideas of our previous work [4], namely the notion of asymptotic correctability, to d-dimensional quantum systems, where d is a prime. We determined a criterion for asymptotic correctability and applied it to $B_n^{(d)}$ steps, which yielded an expression for the characteristic exponent $r^{(d)}$ related to asymptotic $B_n^{(d)}$-correctability. Applying this condition to cryptographic protocols yielded lower bounds for maximum tolerable error rates and the bound in the case of apparently isotropic channels is tight. The restriction to prime dimension is due to two given facts, namely

- the use of asymmetric CSS codes, for which we use Hamada's quantum Shannon bound (theorem 1), which was only derived for primes; and
- the use of the mixing operation U of section 4.5 to simplify our calculations.

We believe that it is reasonable to assume that Hamada's bound may be extended to prime powers. We further believe that formula (30) also holds, if the mixing operation is not applied, but we were not able to give a rigorous proof for that statement. Even if this is not the case, it might be possible to generalize the mixing operation to prime powers. Provided that these tasks are solved, our results hold for prime power dimensions.

It would also be interesting to know, if there are better bounds on the value of $M = \max\left\{\left|\sum_{j=0}^{d-1} z^{lj} A_{j0}\right| \middle| l \in \mathbb{Z}_d^*\right\}$, if A_{l0} is known for all $l \in \mathbb{Z}_d$ and to infer better bounds on M for the non-isotropic case by using the symmetry relations of two-basis protocols, but both tasks seem to be relatively complicated.

Acknowledgments

This work is supported by the EU within the IP SECOQC. Informative discussions with Georgios M Nikolopoulos are acknowledged. K S Ranade is supported by a graduate-student scholarship of the Technische Universität Darmstadt.

Appendix A. Proof of lemma 1

By definition of the Shannon entropy, it is obvious that it is invariant with respect to any permutation of the ξ_i. Furthermore, we know that it is concave, i.e.

$$H_d(\lambda \cdot \xi + (1-\lambda)\cdot\eta) \geqslant \lambda H_d(\xi) + (1-\lambda) H_d(\eta) \qquad \text{for} \quad \lambda \in [0;1]. \tag{A.1}$$

One now can see that $\xi_{\max}$ can be represented as a convex combination of permutations of ξ, where ξ_0 is left invariant, and, on the other hand, ξ can be constructed by a convex combination of permutations of $\xi_{\min}$. □

Appendix B. Proof of lemma 2

A Taylor expansion of H_d up to second order around g yields

$$H_d(p) = 1 + \sum_{i=0}^{d-1}\left(1 - \frac{1}{\ln d}\right)(p_i - g_i) - \frac{d}{2\ln d}\sum_{i=0}^{d-1}(g_i - p_i)^2 + R_2(p). \tag{B.1}$$

Due to the fact that we only consider probability distributions p, the first-order term vanishes and the second-order term can be written in the form of lemma 2 using $K := d/(2\ln d)$. The remainder term $R_2(p)$ can be calculated by Lagrange's formula, i.e.

$$R_2(p) = \sum_{i=0}^{d-1} \frac{\tilde{p}_i^{-2}}{3!\cdot \ln d}(p_i - g_i)^3 \tag{B.2}$$

for some set $\tilde{p}_i$, where $p_i \leqslant \tilde{p}_i \leqslant 1/d$ or $1/d \leqslant \tilde{p}_i \leqslant p_i$ holds for any i. By assumption, we have $\tilde{p}_i \geqslant f/d$; this yields

$$|R_2(p)| \leqslant \sum_{i=0}^{d-1} \frac{(f/d)^{-2}}{3!\cdot \ln d}|p_i - g_i|^3 = K' \|p - g\|_3^3 \tag{B.3}$$

for $K' := d^2 \cdot (3! f^2 \cdot \ln d)^{-1}$, which concludes the proof. □

Appendix C. Proof of theorem 3

In this section, we give the proof of theorem 3, which closely follows the ideas presented in [12]. The main idea in the proof is that the phase propagation can be seen as a convolution, which can be calculated by a sequence of Fourier transform, multiplication and inverse Fourier transform.

The proof is done by induction, which (the case $n = 1$ being obvious) we start for $n = 2$. Consider $(A_{lm})_{lm}, (B_{st})_{st} \in \mathcal{S}_{\mathrm{bd}}^{(d)}$ and denote $(l, m) := |\Psi_{lm}\rangle\langle\Psi_{lm}|$. Applying steps (i) and (ii) of a $B_n^{(d)}$ step in this case yields

$$\rho = \sum_{l,m} A_{lm}(l,m) \otimes \sum_{s,t} B_{st}(s,t) = \sum_{l,m,s,t} A_{lm}B_{st}(l,m)\otimes(s,t) \tag{C.1}$$

$$\overset{\text{GBXOR}}{\mapsto} \sum_{l,m,s,t} A_{lm}B_{st}(l\oplus s, m)\otimes(s, m\ominus t). \tag{C.2}$$

Considering only the case where $m \ominus t = 0$ and tracing out the second pair further yields

$$N_2^{-1}\sum_{l,m,s} A_{lm}B_{sm}(l\oplus s, m) = \sum_{lm}\left[N_2^{-1}\sum_{l'} A_{lm}B_{l\ominus l', m}\right](l,m), \tag{C.3}$$

where $N_2 = \sum_m \left[\left(\sum_l A_{lm}\right)\left(\sum_l B_{lm}\right)\right]$ is the normalization constant. We assume now that the theorem is true for all numbers up to a fixed value n and proceed via induction: let $\rho^{(i)} = \left(A^{(i)}_{lm}\right)^{d-1}_{l,m=0}$ be mixtures of Bell states for $i \in \{1, \ldots, n+1\}$. The outcome of a $B^{(d)}_n$ step applied to the states $1, \ldots, n$ shall be denoted as $\rho' = (A'_{lm})^{d-1}_{l,m=0}$ with normalization constant N_n, the outcome of a $B^{(d)}_{n+1}$ on all $n+1$ states shall be $\rho'' = (A''_{lm})^{d-1}_{l,m=0}$. We calculate

$$A''_{lm} = \frac{1}{dN_2} \sum_i z^{-il} \left[\left(\sum_j z^{ij} A'_{jm} \right) \left(\sum_{j'} z^{ij'} A^{(n+1)}_{j'm} \right) \right] \tag{C.4}$$

$$= \frac{1}{d^2 N_2 N_n} \sum_i z^{-il} \left[\sum_{i',j} z^{ij+i'j} \prod_{k=1}^{n+1} \left(\sum_{j'} z^{i'j'} A^{(k)}_{j'm} \right) \right] \tag{C.5}$$

$$= \frac{1}{d^2 N_2 N_n} \sum_{i,i',j} z^{i(j-l)+i'j} \prod_{k=1}^{n+1} \left(\sum_{j'} z^{i'j'} A^{(k)}_{j'm} \right), \tag{C.6}$$

where N_2 is the normalization constant for a $B^{(d)}_n$ step with $n = 2$ applied to ρ' and $\rho^{(n+1)}$. Using $\sum_{i=0}^{d-1} z^{i(j-l)} = d\delta_{j,l}$, this implies the assertion, if the normalization constant is correct. This can be verified by direct calculation. □

References

[1] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[2] Gottesman D and Lo H K 2003 *IEEE Trans. Inf. Th.* **49** 457
[3] Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098
Steane A M 1996 *Proc. R. Soc. (London)* A **452** 2551
[4] Ranade K S and Alber G 2006 *J. Phys. A: Math. Gen.* **39** 1701–16
[5] Acin A *et al* 2006 *Phys. Rev.* A **73** 012327
[6] Chau H F 2002 *Phys. Rev.* A **66** 060302
[7] Chau H F 2005 *IEEE Trans. Inf. Theory* **51** 1451–68
[8] Nikolopoulos G M and Alber G 2005 *Phys. Rev.* A **72** 032320
[9] Nikolopoulos G M, Ranade K S and Alber G 2006 *Phys. Rev.* A **73** 032325
[10] Hamada M 2004 *J. Phys. A: Math. Gen.* **37** 8303–28
[11] Alber G, Delgado A, Gisin N and Jex I 2001 *J. Phys. A: Math. Gen.* **34** 8821–33
[12] Martín-Delgado M A and Navascués M 2003 *Eur. Phys. J.* D **27** 169–80