Journal of Physics A: Mathematical and General

# Asymptotic correctability of Bell-diagonal quantum states and maximum tolerable bit-error rates

To cite this article: Kedar S Ranade and Gernot Alber 2006 *J. Phys. A: Math. Gen.* **39** 1701

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

J. Phys. A: Math. Gen. **39** (2006) 1701–1716 doi:10.1088/0305-4470/39/7/014

# Asymptotic correctability of Bell-diagonal quantum states and maximum tolerable bit-error rates

**Kedar S Ranade and Gernot Alber**

Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Germany

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

Received 6 October 2005, in final form 22 December 2005
Published 1 February 2006
Online at stacks.iop.org/JPhysA/39/1701

**Abstract**
The general conditions are discussed which quantum state purification protocols have to fulfil in order to be capable of purifying Bell-diagonal qubit-pair states, provided they consist of steps that map Bell-diagonal states to Bell-diagonal states and they finally apply a suitably chosen Calderbank–Shor–Steane code to the outcome of such steps. As a main result a condition on asymptotic correctability is presented, which relates this problem to the magnitude of a characteristic exponent governing the relation between bit and phase errors under the purification steps. This condition allows a straightforward determination of maximum tolerable bit-error rates of quantum key distribution protocols whose security analysis can be reduced to the purification of Bell-diagonal states.

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

## 1. Introduction

The quantum cryptographic protocol developed by Bennett and Brassard (BB84) [1] demonstrates in an impressive way how the key distribution problem of classical cryptography can be solved by means of quantum physics. Later Shor and Preskill [2] demonstrated that the security of this quantum key distribution protocol is guaranteed at least up to bit-error rates of approximately 11.0%. Their proof is based on two main ideas. First, it exploits an equivalence between the originally proposed BB84 protocol as a prepare-and-measure protocol and an associated entanglement-based protocol. Second, it reduces the security issue to the capability of purifying Bell-diagonal qubit-pair states with the help of one-way classical communication and Calderbank–Shor–Steane (CSS) codes [3, 4]. Gottesman and Lo [5] extended Shor and Preskill's approach to entanglement purification protocols which involve bit- and phase-error correcting sequences based on classical two-way communication followed by a CSS-based entanglement purification step. This way they were able to raise the maximum tolerable bit-error rate of the BB84 protocol to 18.9%. Later on Chau [6] extended this approach thereby achieving a maximum tolerable bit-error rate of 20%. Motivated by these investigations of Gottesman and Lo in this work general entanglement purification protocols are analysed which imply the security of any quantum key distribution protocol whose security analysis can be reduced to the purification of Bell-diagonal states. The BB84 protocol and the highly symmetric six-state protocol [7] are well-known examples of such quantum key distribution protocols. The general entanglement purification protocols considered are supposed to map Bell-diagonal states to Bell-diagonal states until the Shannon bound guarantees a successful completion of the entanglement purification on the basis of an appropriate CSS encoding and classical one-way communication. A special example thereof is the entanglement purification protocol introduced by Gottesman and Lo, which, in addition, is compatible with a reduction of an entanglement-based quantum key distribution protocol to an associated prepare-and-measure scheme. As a main result a condition on asymptotic correctability of Bell-diagonal qubit-pair states is presented relating the success of such a general entanglement purification protocol to the magnitude of a characteristic exponent, which governs the scaling between bit and phase errors (main theorem). This latter characteristic exponent can be determined in a straightforward way and allows the determination of maximum tolerable bit-error rates of the Bell-diagonal states involved. Applying this general result to entanglement purification protocols of the Gottesman–Lo type, for example, this criterion implies that even without any phase-error correcting steps of the Gottesman–Lo-type secret keys can be generated by the BB84 and six-state quantum cryptographic protocols up to the already known bit-error rates of $1/5 = 20\%$ and $1/2 - 1/(2\sqrt{5}) \approx 27.6393\%$ [6] and that in the absence of phase-error correction no higher bit-error rates are tolerable. Furthermore, numerical evidence is provided that also arbitrary additional sequences of phase-error correcting steps cannot improve on these particular bounds.

This paper is organized as follows: in order to put the general entanglement purification protocols considered in our main theorem into perspective we first of all summarize basic aspects of the entanglement purification protocol of Gottesman and Lo [5] and generalize their original proposal to arbitrary numbers $n$ of qubit pairs. Correspondingly, basic notions together with the generalized bit-error ($B_n$) and phase-error ($P_n$) correcting Gottesman–Lo-type steps are introduced in section 2. In section 3 basic asymptotic properties of these purification steps are analysed for large numbers of qubit pairs. In particular, the exponents characterizing the scaling of the bit and phase errors under $B_n$ and $P_n$ steps are determined. Our main theorem concerning the asymptotic correctability of Bell-diagonal states and its relation to the exponents characterizing bit and phase errors is stated and proved in section 4. Finally, based on this main theorem in section 5 the asymptotic properties of the $B_n$ and $P_n$ steps characterizing Gottesman–Lo-type purification protocols are investigated in more detail. It is shown that bit-error correcting $B_n$ steps alone are already able to guarantee security of the BB84 protocol and the six-state protocol up to maximum bit-error rates of magnitude $1/5$ and $1/2 - 1/(2\sqrt{5})$, respectively. Furthermore, numerical evidence is provided that even arbitrary sequences of phase-error correcting $P_n$ steps cannot improve on these bounds. Based on this evidence these numbers constitute the maximum possible error rates which are tolerable in the BB84 protocol and in the six-state protocol provided error correction and privacy amplification are based on arbitrary sequences of $B_n$ and $P_n$ steps of the Gottesman–Lo type. For the sake of a clearer presentation of the main ideas some proofs of theorems stated in these sections are postponed to the appendices. A more detailed elaboration of some statements can be found in [8].

## 2. Purification protocols of the Gottesman–Lo type

In this section basic properties of bit-error ($B_n$) and phase-error ($P_n$) correction steps are discussed which generalize the bit- and phase-error correcting steps $B_{\rm GL}$ and $P_{\rm GL}$ proposed by Gottesman and Lo [5] to arbitrary numbers $n$ of qubit pairs. These steps are capable of reducing the bit and phase errors of Bell-diagonal qubit-pair states and can be used as building blocks of entanglement purification protocols which are based on classical two-way communication. In view of the Gottesman–Lo theorem [5] entanglement purification protocols consisting of these $B_n$ and $P_n$ steps can be reduced to prepare-and-measure schemes.

Gottesman and Lo proved that it is sufficient for guaranteeing security of the BB84 and the six-state protocol to be able to purify classical mixtures of the four (pure) Bell states

$$|\Phi^{\pm}\rangle := (1/\sqrt{2})[|00\rangle \pm |11\rangle], \qquad |\Psi^{\pm}\rangle := (1/\sqrt{2})[|01\rangle \pm |10\rangle]. \tag{1}$$

If necessary, the following notation will be used [9]: $(0, 0) := |\Phi^+\rangle$, $(1, 0) := |\Phi^-\rangle$, $(0, 1) := |\Psi^+\rangle$, $(1, 1) := |\Psi^-\rangle$. Here, the numbers are to be understood as elements of the binary field $\mathbb{F}_2$. Mixtures of Bell states are denoted by

$$(a, b, c, d) := a|\Phi^+\rangle\langle\Phi^+| + b|\Phi^-\rangle\langle\Phi^-| + c|\Phi^+\rangle\langle\Phi^+| + d|\Phi^-\rangle\langle\Phi^-| \tag{2}$$

with $a, b, c, d \geqslant 0$ and $a + b + c + d = 1$. The set of all such Bell-diagonal states is denoted by $\mathcal{S}_{\rm bd}$. A Bell-diagonal state is entangled if and only if one of the four coefficients is larger than 1/2 [9]. In our discussion a Bell-diagonal state will be called entangled with respect to $|\Phi^+\rangle$ if $a > 1/2$. The set of states with $a > 1/2$ and with $a \geqslant 1/2$ are denoted by $\mathcal{S}_{\rm v}$ and by $\overline{\mathcal{S}_{\rm v}}$, respectively.

In the subsequent discussion we choose the state $|\Phi^+\rangle$ as the reference state for entanglement purification; therefore $a \equiv F$ will be called fidelity (with respect to $|\Phi^+\rangle$). Furthermore, the parameters $b$, $c$ and $d$ are the pure phase-error rate, the pure bit-error rate and the combined bit-phase-error rate. Correspondingly, the parameters $B = c + d$ and $P = b + d$ are the total bit- and phase-error rates.

For the purposes of entanglement purification it is sufficient to assume that Alice and Bob share an infinite number of qubit pairs, all described by the same density operator $\rho = (a, b, c, d) \in \mathcal{S}_{\rm v}$ [5, 10, 11]. All purification steps considered act as mappings on the set $S_{\rm bd}$. A particular step of the purification protocols considered takes a fixed number $n$ of qubit pairs, all prepared in the same state $\rho = (a, b, c, d)$, as input and yields with some non-vanishing probability, which may depend upon $\rho$, a final qubit pair in the state $\rho' = (a', b', c', d')$ or no qubit pair at all.

### 2.1. $B_n$ steps

A $B_n$ step which involves $n \in \mathbb{N}$ qubit pairs reduces the bit-error rate, but simultaneously it also increases the phase-error rate of the original quantum state. It is defined by the following sequence of steps.

(i) Alice and Bob choose $n$ qubit pairs $QP_1, \ldots, QP_n$.
(ii) Alice and Bob apply bilateral BXOR operations of the form BXOR$(QP_1, QP_k)$ for all qubit pairs $k \in \{2, \ldots, n\}$ ($n - 1$ operations).
(iii) Alice and Bob measure the bit parities of all pairs from $QP_2$ to $QP_n$ and continue using $QP_1$ if and only if all parities are +1 (same bit values for Alices and Bobs measurement). The pairs $QP_2, \ldots, QP_n$ are discarded.

Here, the BXOR operation on Bell-diagonal states is defined by [5, 9]

$$\mathrm{BXOR}(QP_1, QP_2) : (l_1, m_1) \otimes (l_2, m_2) \mapsto (l_1 \oplus l_2, m_1) \otimes (l_2, m_1 \oplus m_2). \tag{3}$$

Thus, for a given set of $n$ pure Bell pairs $(l_i, m_i)$, according to step (ii) the BXOR operations are equivalent to the transformation

$$\bigotimes_{i=1}^{n} (l_i, m_i) \mapsto \left(\bigoplus_{i=1}^{n} l_i, m_1\right) \otimes \left[\bigotimes_{k=2}^{n} (l_k, m_1 \oplus m_k)\right]. \tag{4}$$

According to step (iii) the pair $QP_1$ is kept for the next step, if $m_1 \oplus m_k = 0$ holds for all $k \in \{2, \ldots, n\}$. Otherwise this qubit pair is discarded. Therefore, we obtain the relations $B_1 = \mathrm{id}_{\mathcal{S}_{\mathrm{bd}}}$, $B_2 = B_{\mathrm{GL}}$, $B_n B_m = B_{nm}$ and $(B_{\mathrm{GL}})^n = B_{2^n}$.

Note that Alice and Bob could perform the measurements of the pairs $QP_2, \ldots, QP_n$ immediately after the respective BXOR operation. If the pair $QP_1$ is discarded immediately after the first false parity, the average number of discarded qubits reduces, which results in a higher key generation rate.

In appendix A.1 it is shown that with respect to the first qubit pair $QP_1$ a $B_n$ step can be identified with a mapping $B_n : \mathcal{S}_{\mathrm{bd}} \to \mathcal{S}_{\mathrm{bd}}$ with $B_n : (a, b, c, d) \mapsto (a', b', c', d')$ and with

$$\begin{aligned} a' &= [(a+b)^n + (a-b)^n]/2N, & b' &= [(a+b)^n - (a-b)^n]/2N, \\ c' &= [(c+d)^n + (c-d)^n]/2N, & d' &= [(c+d)^n - (c-d)^n]/2N. \end{aligned} \tag{5}$$

The value $N = [(a+b)^n + (c+d)^n]$ is the survival probability of the first pair.

### *2.2. $P_n$ steps*

In analogy to the $B_{\mathrm{GL}}$ step also the $B_n$ step can be adapted to correct phase errors [5]. However, according to the Gottesman–Lo theorem such a step has the disadvantage that it cannot be reduced to some prepare-and-measure protocol. Therefore, Gottesman and Lo originally developed an alternative phase-error correction step which is not as efficient, but which can be reduced to a prepare-and-measure protocol. The $P_n$ step considered in the following is a generalization of this step originally developed by Gottesman and Lo [5]. For any $n \in \mathbb{N}_0$, we define a $P_{2n+1}$ step as follows.

(i) Alice and Bob choose $2n+1$ qubit pairs $QP_1, \ldots, QP_{2n+1}$.
(ii) Alice and Bob perform Hadamard transformations [5, 12] on all pairs.
(iii) Alice and Bob perform BXOR operations of the form $\mathrm{BXOR}(QP_1, QP_k)$ for all qubit pairs with $k \in \{2, \ldots, 2n+1\}$ ($2n$ operations).
(iv) Alice and Bob measure the bit parities of all pairs from $QP_2$ to $QP_{2n+1}$; the number of pairs with bit parity $-1$ (different outcomes for Alice and Bob) is denoted as $m \in \{0, \ldots, 2n\}$.
(v) Alice and Bob perform a Hadamard transformation on $QP_1$.
(vi) If $m \geqslant n+1$, Bob performs the transformation $\mathbb{I} \otimes \sigma_z$ on the first pair. Otherwise, Bob leaves the first pair unchanged. The pairs $QP_2, \ldots, QP_{2n+1}$ are discarded.

If in step (v) Alice and Bob apply the Hadamard transformation to all qubit pairs, they can exchange steps (iv) and (v), if they measure the phase parity $l_1 \oplus l_k$ instead of the bit parity for $k \in \{2, \ldots, 2n+1\}$. In this latter case the transformation yields

$$\bigotimes_{i=1}^{2n+1} (l_i, m_i) \mapsto \left(l_1, \bigoplus_{i=1}^{2n+1} m_i\right) \otimes \left[\bigotimes_{k=2}^{2n+1} (l_1 \oplus l_k, m_k)\right]. \tag{6}$$

According to Bob's final transformation in step (vi) the new phase of the first qubit pair $QP_1$, as characterized by the parameter $l_1$, is fixed by the majority of the $2n+1$ phases of all qubit pairs involved.

Similar to the case of the $B_n$ step, we obtain $P_1 = \mathrm{id}_{\mathcal{S}_{\mathrm{bd}}}$ and $P_3 = P_{\mathrm{GL}}$. But contrary to the case of $B_n$ steps, a sequence $P_n P_m$ is always worse than a single $P_{nm}$ step. This originates from the fact that the bit-errors introduced by $P_n P_m$ and $P_{nm}$ sequences are always equal, whereas the majority of majorities is not necessarily the total majority of phases. Note that the use of a $P_n$ step is equivalent to the application of the $[n, 1, n]$ code in [6].

Calculating the evolution resulting from the application of a $P_n$ step is much more complicated than the resulting evolution of $B_n$ steps as given in (5). However, it turns out that the evolution of bit and phase errors $B$ and $P$ can be determined easily (compare with (15)).

### 2.3. Remarks

Note that the bit-error rates after applying $B_n$ or $P_n$ steps depend only on the previous bit-error rate (but not on the phase-error rate); similarly, the new phase-error rate after using a $P_n$ step depends only on the previous phase-error rate. Using $B_n$ steps, the exact coefficients determine the evolution of the phase-error rate; considering $\rho \in \mathcal{S}_{\rm v}$ and $n \to \infty$, the evolution is mostly determined by the fidelity $a$ and the pure phase-error rate $b$.

In particular, when using $B_n$ and $P_n$ steps only, Alice and Bob do not gain any advantage, if they measure bit errors after performing some of these steps. This seems to be obvious considering the fact that they can be reduced to prepare-and-measure schemes, where phase errors cannot have any influence on the protocol.

## 3. Asymptotic evolution of $B_n$ and $P_n$ steps

In this section the evolution of Bell-diagonal qubit-pair states is investigated if they are subjected to $B_n$ and $P_n$ steps. Here, the asymptotic evolution for large values of $n$ is of particular interest. In the subsequent discussion this asymptotic evolution is characterized by exponents $r$ and $r_P$ for $B_n$ and $P_n$ steps, respectively, which determine the relative scaling between bit and phase errors. As demonstrated in detail in section 4 the values of these characteristic exponents are directly related to the correctability of Bell-diagonal quantum states.

### 3.1. Asymptotic evolution of $B_n$ steps

Let us consider the evolution of the quantum state $\rho = (a, b, c, d) \in \mathcal{S}_{\rm v}$ of a single qubit pair using $B_n$ steps for large values of $n$. For the sake of simplicity it is assumed that $b > 0$ and $c + d > 0$, because the remaining cases are trivial. For this purpose we define first of all some useful variables:

$$\tilde{x} := \frac{a+b}{c+d}, \qquad \Delta_1 := \frac{a-b}{c+d}, \qquad \Delta_2 := \frac{c-d}{c+d}. \tag{7}$$

After having performed a $B_n$ step the resulting quantum state is given by

$$(a', b', c', d') \equiv \left(\tfrac{1}{2} - x_n + y_n + \delta_n, \tfrac{1}{2} - y_n - \delta_n, x_n - \delta_n, \delta_n\right) := B_n[(a, b, c, d)], \tag{8}$$

where $x_n$ and $y_n$ denote the resulting *bit-error rate* ($B$) and *inverse phase-error rate* $(1/2 - P)$. The quantity $\delta_n$ is the joint bit-phase-error rate as determined by (5). Its explicit form will not be used in the following. The evolution (5) immediately implies (the symbol $\doteq$ means asymptotically equal)

$$x_n = (1 + \tilde{x}^n)^{-1} \doteq \tilde{x}^{-n}, \qquad 2y_n = \left(\Delta_1^n + \Delta_2^n\right) / (1 + \tilde{x}^n) \doteq \Delta_1^n / \tilde{x}^n. \tag{9}$$

For particular values of the parameters $a, b, c, d$ it is possible to define a characteristic exponent $r \in \mathbb{R}$ with the defining property $\lim_{n\to\infty} x_n/(2y_n)^r = 1$. In view of the elementary relation

$$\frac{x_n^{1/r}}{2y_n} = \frac{(1+\tilde{x}^n)^{1-1/r}}{\Delta_1^n + \Delta_2^n} \doteq \frac{\tilde{x}^{n(1-1/r)}}{\Delta_1^n} = \left(\frac{\tilde{x}^{1-1/r}}{\Delta_1}\right)^n, \tag{10}$$

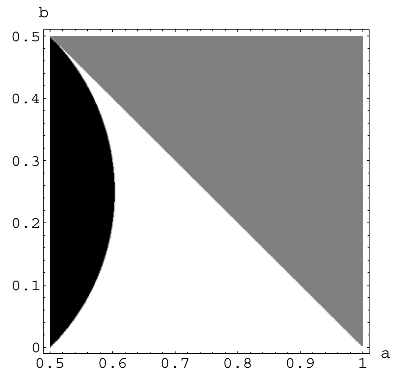


**Figure 1.** Regions for $r > 2$ (white) and $1 \leqslant r \leqslant 2$ (black) for fidelity $a$ and pure phase-error rate $b$; grey: no physical states.

this defining property implies that the term in the bracket must be unity, i.e.

$$\tilde{x}^{(1-1/r)} = \Delta_1 \Leftrightarrow r = \left[1 - \frac{\ln \Delta_1}{\ln \tilde{x}}\right]^{-1} = \frac{\ln \frac{a+b}{c+d}}{\ln \frac{a+b}{a-b}}. \tag{11}$$

Therefore, using the conservation of probability, i.e. $c + d = 1 - a - b$, one may establish relations between values of the characteristic parameter $r$ and particular Bell-diagonal states. Two examples of such correlations are

$$\begin{aligned} r > 1 \quad &\Leftrightarrow \quad a > 1/2 \text{ (entanglement w.r.t. } |\Phi^+\rangle), \\ r > 2 \quad &\Leftrightarrow \quad f(a, b) := a^2 + b^2 - (a + b)/2 > 0 \\ &\Leftrightarrow \quad (a - 1/4)^2 + (b - 1/4)^2 > (1/2\sqrt{2})^2 = 1/8. \end{aligned} \tag{12}$$

The left-hand side of the latter inequality can be interpreted geometrically as a cylinder centred around the chaotic state $\rho = \frac{1}{4}\,\mathbb{I}$ (compare with figure 1). The function $f$ is easier to evaluate than the exponent $r$ and will be used in some calculations. In the main theorem of the next chapter it will be demonstrated that purification succeeds in the regime of characteristic exponents $r > 2$.

### *3.2. Asymptotic evolution of $P_n$ steps*

The evaluation of the asymptotic evolution of $P_n$ steps turns out to be much more complicated than that of $B_n$ steps. For this purpose the following lemma is useful:

**Lemma 1** (Properties of the binomial distribution)**.** *Let $p \in [1/2; 1]$, $n \in \mathbb{N}$ be odd; in these cases the relation*

$$f_n(p) := \sum_{k=0}^{(n-1)/2} \binom{n}{k} p^k (1-p)^{n-k} = c(n, p) z^n \tag{13}$$

*is valid with $z := 2\sqrt{p(1-p)}$, where the image of the function $c(n, p)$ is contained in the interval $[0; 1]$ and $c(n, p)$ decreases at most sub-exponentially for $n \to \infty$ and for any $p \in [1/2; 1]$.*

**Proof.** A proof of this lemma is given in appendix B.1. □

Analogous to (8) the asymptotic evolution of the state $(a, b, c, d)$ of a qubit pair under a $P_n$ step is given by

$$(a', b', c', d') = \left(\tfrac{1}{2} - u_n + v_n + \varepsilon_n, u_n - \varepsilon_n, \tfrac{1}{2} - v_n - \varepsilon_n, \varepsilon_n\right) := P_n[(a, b, c, d)]. \tag{14}$$

Here, $u_n$ is the *phase-error rate* and $v_n$ is the *inverse bit-error rate*. The value $\varepsilon_n$ is the joint bit-phase-error rate, which is given in appendix A.2, but which will not be used in the following.

Using these definitions, the calculation of $u_n$ and $v_n$ is straightforward, whereas the calculation of the correlation $\varepsilon_n$ is rather involved. For odd values of $n \in \mathbb{N}$ one obtains the relations

$$\begin{aligned} u_n &= \sum_{k=0}^{(n-1)/2} \binom{n}{k} (a+c)^k (b+d)^{n-k} \overset{\text{Lemma1}}{\leqslant} [4(a+c)(b+d)]^{n/2}, \\ 2v_n &= (a+b-c-d)^n \equiv F^n. \end{aligned} \tag{15}$$

Using lemma 1 we may also write $u_n = c(n, a+c)z^n$ for $z = 2\sqrt{(a+c)(b+d)}$. Similar to the construction for $B_n$ steps, one can define an exponent $r_P$, which characterizes the asymptotic evolution of $P_n$ in the sense that $z/F^{r_P} = 1$. This yields the relation

$$r_P = \frac{\ln z}{\ln F} = \frac{\ln 2\sqrt{(a+c)(b+d)}}{\ln(a+b-c-d)} = \frac{1}{2}\frac{\ln 4(a+c)(b+d)}{\ln(a+b-c-d)} \tag{16}$$

for the characteristic exponent $r_P$. In view of the relation

$$\frac{u_n}{(2v_n)^{r_P}} = \frac{c(n, a+c)z^n}{F^{r_P n}} = c(n, a+c)\left(\frac{z}{F^{r_P}}\right)^n, \tag{17}$$

the quotient $u_n/(2v_n)^{r_P}$ converges to $+\infty$ for all exponents larger than $r_P$ because $c(n, a+c) \leqslant 1$ decreases at most sub-exponentially. Furthermore, the bounds $z, F \leqslant 1$ imply the inequalities ($B$ and $P$ denote bit and phase-error rate):

$$\begin{aligned} r_P > 1 \quad &\Leftrightarrow \quad (1/2 - B)^2 + (1/2 - P)^2 > (1/2)^2 = 1/4, \\ r_P > 2 \quad &\Leftrightarrow \quad (1 - 2B)^4 - 4P(1 - P) > 0. \end{aligned} \tag{18}$$

### *3.3. Remarks*

Note that the $P_n$ step defines a mapping $P_n : (B, P) \mapsto (B', P')$, if one ignores the correlation between bit and phase errors. In particular, a possible statistical independence of bit and phase errors, i.e. the validity of the relation $(b+d)(c+d) - d = 0$, is invariant under $P_n$ steps but not under $B_n$ steps. The following lemma is of some interest:

**Lemma 2** (Separability using $P_n$ steps)**.** *Let $\rho = (a, b, c, d) \in \mathcal{S}_\text{V}$, $n \in \mathbb{N}$ be odd and $\rho' = (a', b', c', d') := P_n(\rho)$; this implies*

*(i) $\rho'$ is entangled if and only if $a' > 1/2$ holds.*

*(ii) If bit and phase-error rates in $\rho$ are statistically independent, then for sufficiently large $n$ the state $\rho'$ is separable if and only if $r_P(\rho) < 1$ holds.*

**Proof.** For the proof of the first statement, it is sufficient to show that $b', c', d' \leqslant 1/2$. From (15) follows the inequality $B' = c' + d' = (1 - F^n)/2 < 1/2$ and from $F > 0$ we obtain $c', d' \leqslant 1/2$. The value $P' = b' + d'$ decreases monotonically in $n$, which by $b, c, d \leqslant 1/2$ implies the assertion.

Thus, for the proof of the second inequality one concentrates on the value of $a'$. Statistical independence of bit and phase errors implies $a' = 1 - P' - B' + B'P'$; using the notation

$c(n) := c(n, a+c)$ yields $a' = 1 - c(n)z^n - (1/2 - F^n/2) + c(n)z^n(1/2 - F^n/2)$ and $a' \leqslant 1/2 \Leftrightarrow (1 - c(n)z^n)F^n \leqslant c(n)z^n$. Therefore, for a resulting separable state for $n \to \infty$, $F^n \leqslant c(n)z^n$ is sufficient. Because $c(n)$ decreases at most sub-exponentially, $F < z$, i.e. $r_P < 1$ is sufficient. On the other hand, if $r_P \geqslant 1$, i.e. $F \geqslant z$, the assertion follows by a similar reasoning. □

## 4. The criterion for asymptotic correctability (main theorem)

In this section the question of asymptotic correctability of Bell-diagonal quantum states is addressed from a more general point of view. In particular, our main theorem is stated and proved which relates the asymptotic correctability of a large class of general entanglement purification protocols to the characteristic exponents determining the scaling of their resulting bit and phase errors. The general entanglement purification protocols of this class are supposed to consist of arbitrary sequences of basic steps which involve classical one- and/or two communication between Alice and Bob until the Shannon bound is reached. Subsequently these steps are supposed to be completed by a CSS-based purification protocol, which involves classical one-way communication. This main theorem will be specialized to sequences of $B_n$ and $P_n$ steps in the next section.

Let us start by defining the notion of *asymptotic correctability*:

**Definition 1** (Asymptotic correctability). *Let $\rho = (a, b, c, d) \in \mathcal{S}_{\mathrm{v}}$ and $(S_n)_{n\in\mathbb{N}}$ be a sequence of possible steps in an entanglement purification protocol. The state $\rho$ is called asymptotically $S_n$-correctable under this sequence if there exists an $N_0 \in \mathbb{N}$ such that for all $n \in \mathbb{N}, n \geqslant N_0$, the inequality* $\mathrm{AsymCSS}[S_n(\rho)] := 1 - H(B) - H(P) > 0$ *holds, where B and P denote bit and phase-error rates of the resulting state $S_n(\rho)$ after the use of that step.*

Here, $H(\xi) := -\xi\log_2\xi - (1-\xi)\log_2(1-\xi)$ is the binary Shannon entropy and the function AsymCSS denotes the Shannon bound, i.e. the minimum rate of an asymmetric CSS code [3, 4]. If $\mathrm{AsymCSS}(\rho)$ is positive the state $\rho$ can be corrected by some CSS code, i.e. by one-way classical communication. Important special cases are $(S_n)_{n\in\mathbb{N}} \in \{(B_n)_{n\in\mathbb{N}}, (P_{2n+1})_{n\in\mathbb{N}_0}\}$. Note that asymptotic correctability implies correctability, but not vice versa, in general.

Using the notation of (8) for the state of a qubit pair after application of an arbitrary $S_n$ step, i.e. $B \to x_n$ and $P \to 1/2 - y_n$, one obtains

$$\mathrm{AsymCSS}(x_n, 1/2 - y_n) = -H(x_n) + (\ln 2)^{-1}\left[2y_n \operatorname{artanh}(2y_n) + \tfrac{1}{2}\ln\left(1 - 4y_n^2\right)\right]. \quad (19)$$

Because of the symmetry of AsymCSS, this is also valid for the case, where $P \to x_n$ and $B \to 1/2 - y_n$. Dropping positive terms in the (partial) Taylor series expansion of (19) one obtains the lower bound

$$\mathrm{AsymCSS}(x_n, 1/2 - y_n) \geqslant A(x_n, y_n) := (\ln 2)^{-1}\left[x_n \ln x_n - x_n + 2y_n^2\right] \quad (20)$$

for $0 \leqslant x_n \leqslant 1/2$ and $0 \leqslant y_n \leqslant 1/2$.

Obviously, one can define an *asymptotic $S_n$-correction* purification protocol in the following way: Alice and Bob determine the smallest $n \in \mathbb{N}$, such that $S_n(\rho)$ can be corrected by some asymmetric CSS code, apply $S_n$ and use an appropriate CSS code to obtain a purified final state. In the case of $B_n$ and $P_n$ steps smaller values of $n$ usually result in higher key generation rates, both in the two-way part of the protocol and in the CSS part.

Finally, it should be noted that the condition $\mathrm{AsymCSS}(\rho) > 0$ is only sufficient, but not necessary for the existence of asymmetric CSS codes which are capable of purifying a quantum state. If this condition is violated, there may also exist applicable CSS codes, but this cannot be guaranteed in general.

After these introductory remarks let us state and prove now the following main theorem:

**Theorem 1** (Main theorem). *Let $\rho = (a, b, c, d) \in \mathcal{S}_v$ and $(S_n)_{n\in\mathbb{N}}$ be a sequence of possible steps in an entanglement purification protocol. Furthermore, let*

$$(x_n, y_n) = (B, 1/2 - P) \quad \textit{or} \quad (x_n, y_n) = (P, 1/2 - B)$$

*after application of an $S_n$ step, and let $(S_n)_{n\in\mathbb{N}}$ be a sequence of such steps, such that* $\lim_{n\to\infty} x_n = 0$ *holds. Finally, let*

$$r_{\text{sup}} := \sup\left\{r \in \mathbb{R} \middle| \sup\left\{x_n \middle/ y_n^r \middle| n \in \mathbb{N}\right\} < \infty\right\}. \tag{21}$$

*Then, $\rho$ is asymptotically $S_n$-correctable if $r_{\text{sup}} > 2$ holds. If $r_{\text{sup}} < 2$ holds, then $\rho$ is not asymptotically $S_n$-correctable. In the case where $r_{\text{sup}} = 2$, no general statement can be made.*

Before starting with the proof, it is worth noting that the characteristic exponent $r_{\text{sup}}$ is chosen in such a way that it generalizes the exponents $r$ and $r_P$ of sections 3.1 and 3.2 (see also corollary 1). In particular, it measures the relative behaviour of $x_n$ and $y_n$. The condition $r_{\text{sup}} > 2$ can be interpreted as saying that the error rate $x_n$ has to converge more than quadratically faster to zero than the other rate, namely $1/2 - y_n$, converges to 1/2.

**Proof of the theorem.** First part ($r_{\text{sup}} > 2$ is sufficient): if $r_{\text{sup}} > 2$, one can find an exponent $r > 2$ and a value $c > 0$, such that $x_n \leqslant c y_n^r$ for all $n \in \mathbb{N}$. The function $A(x, y)$ is used to minorize $\text{AsymCSS}(x, 1/2 - y)$. As a consequence the worst case with the maximum possible error rates is given by $x_n = c y_n^r$. This implies

$$\begin{aligned}(\ln 2 \cdot A)(x_n, y_n) &= c y_n^r \ln\left(c y_n^r\right) - c y_n^r + 2y_n^2 > 0\\ \Leftrightarrow\ & \frac{c}{2} y_n^{r-2}[(\ln c + 1) + r \ln y_n] + 1 > 0.\end{aligned} \tag{22}$$

Because $x_n$ tends to zero in the limit $n \to \infty$, also $y_n$ does so. Therefore, the first term of the latter inequality becomes arbitrarily small due to $\lim_{n\to\infty} y_n^{r-2} \ln y_n = 0$. Thus, we obtain the required result, namely that $\text{AsymCSS}(x_n, 1/2 - y_n) > 0$ for large $n$.

Second part ($r_{\text{sup}} \geqslant 2$ is necessary): the condition $r_{\text{sup}} < 2$ implies that $\sup\left\{x_n \middle/ y_n^2 \middle| n \in \mathbb{N}\right\} = \infty$, i.e. there exists at least a subsequence, for which $c := \inf\left\{x_n \middle/ y_n^2 \middle| n \in \mathbb{N}\right\} > 0$ holds. From the Shannon bound it is obvious that for guaranteeing correctability, $x_n$ should be as small and $y_n$ as large as possible. Therefore, in view of the conditions of the theorem the best case is given by a subsequence with $x_n = c y_n^2$. Using relation (19) and the elementary properties

$$\begin{aligned}&(\mathrm{d}/\mathrm{d}y)[2y\,\text{artanh}(2y) + \ln(1 - 4y^2)/2] = 2\,\text{artanh}(2y),\\ &(\mathrm{d}/\mathrm{d}y)[2\,\text{artanh}(2y)] = 4/(4 - y^2),\\ &(\mathrm{d}/\mathrm{d}y)[-\ln 2 H(cy^2)] = 2cy \ln(cy^2/(1 - cy^2)),\\ &(\mathrm{d}^2/\mathrm{d}y^2)[-\ln 2 H(cy^2)] = 2c[\ln(cy^2/(1 - cy^2)) - 2/(cy^2 - 1)],\end{aligned} \tag{23}$$

one therefore notices

$$\begin{aligned}&\lim_{n\to\infty} \text{AsymCSS}\left(c y_n^2, 1/2 - y_n\right) = 0,\\ &\lim_{n\to\infty} \frac{\mathrm{d}}{\mathrm{d}y} \text{AsymCSS}(cy^2, 1/2 - y)|_{y=y_n} = 0,\\ &\frac{\mathrm{d}^2}{\mathrm{d}y^2} \text{AsymCSS}(cy^2, 1/2 - y)|_{y=y_n} < 0 \quad \text{for} \quad y_n \to 0.\end{aligned} \tag{24}$$

Thus, the state is not asymptotically $S_n$-correctable and the assertion is proved. □

In particular, the special case $(S_n)_{n\in\mathbb{N}} \in \{(B_n)_{n\in\mathbb{N}}, (P_{2n+1})_{n\in\mathbb{N}_0}\}$ yields

**Corollary 1** (Asymptotic $B_n$- and $P_n$-correctability)**.** *For $\rho \in \mathcal{S}_{\mathrm{v}}$ the following statements are true:*

$$\begin{aligned} &\rho \text{ is asymptotically } B_n \text{ correctable} \quad \Leftrightarrow \quad r(\rho) = \frac{\ln\frac{a+b}{c+d}}{\ln\frac{a+b}{a-b}} > 2, \\ &\rho \text{ is asymptotically } P_n \text{ correctable} \quad \Rightarrow \quad r_P(\rho) = \frac{\ln 4(a+c)(b+d)}{2\ln(a+b-c-d)} \geqslant 2. \end{aligned} \tag{25}$$

**Proof.** This assertion follows immediately from theorem 1 and the basic properties of $B_n$ and $P_n$ steps discussed in sections 3.1 and 3.2. The equivalence in the case of asymptotic $B_n$-correctability results from the fact that for $r = 2$ the equation $\lim_{n\to\infty} x_n/y_n^2 = 4$ holds (see section 3.1); this implies $\inf\{x_n/y_n^2 | n \in \mathbb{N}\} > 0$ and the assertion follows as in the proof of theorem 1. □

## 5. Asymptotic correctability using $B_n$ and $P_n$ steps

In this section it is analysed for which qubit-pair states $(a, b, c, d)$ a purification based on $B_n$ and $P_n$ steps and asymmetric CSS codes fulfilling the Shannon bound is possible according to the main theorem of the previous section. It is shown that bit-error correcting $B_n$ steps alone are already able to guarantee security of the BB84 protocol and the six-state protocol up to maximum bit-error rates of magnitudes $1/5$ and $1/2 - 1/(2\sqrt{5})$, respectively. Furthermore, numerical evidence is provided that even arbitrary sequences of phase-error correcting $P_n$ steps cannot improve on these bounds. Based on this evidence the maximum possible bit-error rates which are tolerable in the BB84 protocol and in the six-state protocol are given by $1/5$ and $1/2 - 1/(2\sqrt{5})$, provided error correction and privacy amplification are based on arbitrary sequences of $B_n$ and $P_n$ steps and the use of CSS codes.

### *5.1. Reduction to the use of the exponent r*

So far we have concentrated on three possibilities for purifying a given Bell-diagonal quantum state. A quantum cryptographic protocol can be made secure, if it produces states with $\mathrm{AsymCSS}(\rho) > 0$, $r(\rho) \equiv \frac{\ln\frac{a+b}{c+d}}{\ln\frac{a+b}{a-b}} > 2$ or $r_P(\rho) \equiv \frac{\ln 4(a+c)(b+d)}{2\ln(a+b-c-d)} > 2$ and possibly in the case $r_P(\rho) = 2$. As can be seen from the following theorem these conditions are not independent:

**Theorem 2** (Reduction to the characteristic exponent $r$)**.** *Let $\rho = (a, b, c, d) \in \overline{\mathcal{S}_{\mathrm{v}}}$. Then,*

$$\mathrm{AsymCSS}(\rho) > 0 \Rightarrow r_P(\rho) > 1 \Rightarrow r(\rho) > 2. \tag{26}$$

*In particular, $r_P(\rho) \geqslant 2 \Rightarrow r(\rho) > 2$.*

**Proof.** A detailed proof is given in appendix B.2. □

It should be noted that for any state $\rho \in S_{\mathrm{bd}}$, the value of $r(\rho)$ is invariant with respect to $B_n$ steps, because from (5) one obtains immediately the relation $r[B_n(\rho)] = r(\rho)$.

### *5.2. Limits for the maximum tolerable error rate*

Theorem 2 shows that it is sufficient to consider the characteristic exponent $r$ for determining the correctability using $B_n$ and $P_n$ steps and asymmetric CSS codes (using the Shannon bound).

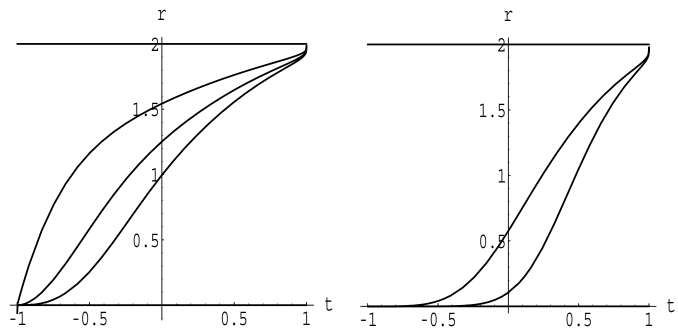


**Figure 2.** The function $r[P_n(K(t))]$ for $n \in \{3, 5, 7\}$ (left) and $n \in \{11, 21\}$ (right). In both diagrams, $n$ increases from top to bottom.

According to this theorem the only possibility of purifying states with $r \leqslant 2$ is to apply $P_n$ steps, which may possibly yield states with $r > 2$. If this is not possible, the asymptotic $B_n$-correction is already optimal with respect to the maximum tolerable error rate in our model. The following conjecture indeed suggests that the asymptotic $B_n$-correction is optimal:

**Conjecture 1** (Optimality of the asymptotic $B_n$-correction)**.** *Let* $\rho = (a, b, c, d) \in \overline{\mathcal{S}_{\rm v}}$ *with* $r(\rho) \leqslant 2$*. Then, for all odd* $n \in \mathbb{N}$

$$r[P_n(\rho)] \leqslant 2. \tag{27}$$

The subsequent lemmata show that for a proof of this conjecture it is sufficient to prove it on a certain subset of states (compare with figure 1). But this turns out to be difficult and an analytical proof is not known. However, as demonstrated below numerical results (compare with figure 2) and plausibility arguments are in favour of the validity of this conjecture.

For the formulation of these lemmata it is convenient to parameterize the set $\mathcal{S}_{\rm v}$ by

$$Z(a, b; z) := (a, b, z(1 - a - b), (1 - z)(1 - a - b)) \in \overline{\mathcal{S}_{\rm v}} \tag{28}$$

with $a \geqslant 1/2, b \geqslant 0, a + b \leqslant 1$ and $z \in [0; 1]$. It is useful to visualize these lemmata with the help of figure 1. The function $f$ introduced in (12) will be used frequently.

**Lemma 3** (Concerning the diagonals in figure 1)**.** *Let* $a, b, z, z', \delta \in [0; 1]$ *be chosen in such a way that* $Z(a, b; z), Z(a - \delta, b + \delta; z') \in \overline{\mathcal{S}_{\rm v}}$*. Then,* $r[Z(a, b; z)] \leqslant 2 \Rightarrow r[Z(a - \delta, b + \delta; z')] \leqslant 2$.

**Proof.** By (12), $r \leqslant 2 \Leftrightarrow f(a, b) \leqslant 0$; thus, $z$ and $z'$ are unnecessary and one can calculate $f(a - \delta, b + \delta) = f(a, b) + 2\delta(-a + b + \delta)$. The first expression is negative by assumption, the factor $2\delta$ is non-negative. Using $Z(a - \delta, b + \delta; z') \in \overline{\mathcal{S}_{\rm v}}$, one finds $a - \delta \geqslant 1/2$ and therefore $\delta \leqslant a - 1/2 \leqslant a - b$, which implies the assertion. □

**Lemma 4** (First reduction to states with $d = 0$)**.** *Let* $a, b \in [0; 1]$ *be chosen in such a way that* $Z(a, b; 1) \in \overline{\mathcal{S}_{\rm v}}$ *and* $f(a, b) \leqslant 0$*, and let* $n \in \mathbb{N}$ *be odd and* $z \in [0; 1]$*. Then,* $r[P_n(Z(a, b; 1))] \leqslant 2 \Rightarrow r[P_n(Z(a, b; z))] \leqslant 2$.

**Proof.** Let $\rho = Z(a, b; z) \in \mathcal{S}_{\rm v}$. The $P_n$ step can be viewed as a mapping from old to new bit and phase-error rates, i.e. $P_n : (B, P) \mapsto (B', P')$. In view of $B = c + d$ and $B' = c' + d'$ the bit-error rates do not depend on $z$. In figure 1 a variation of $z$ results in a variation on the diagonal $a' + b' = \text{constant}$. By the evolution (6) one notes that the fidelity $a'$ becomes larger, if the initial phase-error rate gets small (proof in appendix B.3.1). Lemma 3 now implies the assertion. □

Because of this, it is sufficient to consider the best case, i.e. $z = 1$ or $d = 0$.

**Lemma 5** (Second reduction of the parameter space)**.** *Let $a, b, \varepsilon \in [0; 1]$ be chosen in such a way that $Z(a, b; 1), Z(a - \varepsilon, b + \varepsilon; 1) \in \overline{\mathcal{S}_v}$, and let $n \in \mathbb{N}$ be odd. Then, $r[P_n(Z(a, b; 1))] \leqslant 2 \Rightarrow r[P_n(Z(a - \varepsilon, b + \varepsilon; 1))] \leqslant 2$.*

**Proof.** The bit-error rate $B = c + d$ before and thus after a $P_n$ step does not depend on $\varepsilon$. Using lemma 3, in the best case the fidelity $a'$ is maximal after performing a $P_n$ step; as shown in appendix B.3.2 this is the case for $\varepsilon = 0$. □

Because of lemmata 4 and 5 the assertion from conjecture 1 has to be shown only on a certain subset, which can be parameterized by the function $K : [-1; +1] \to \overline{\mathcal{S}_v}$ with

$$K(t) := Z(1/4 + (2\sqrt{2})^{-1}\cos(\pi t/4), 1/4 + (2\sqrt{2})^{-1}\sin(\pi t/4); 1). \tag{29}$$

This subset corresponds to the border of the black circle of figure 1. Figure 2 demonstrates graphically the validity of the claim for the first few values of $n$. The curves of figure 2 even seem to imply that $r$ tends to zero for large values of $n$. By lemma 2 it also appears that the states become separable and thus non-correctable for large values of $n$.

Provided conjecture 1 is correct the following conjecture can be proven:

**Conjecture 2** (Correctability by using $B_n$ and $P_n$ steps)**.** *For $\rho = (a, b, c, d) \in \mathcal{S}_v$ the following statements are equivalent:*

*(i) $r(\rho) > 2$ (or equivalent $f(a, b) > 0$ by (12));*
*(ii) $\rho$ is asymptotically $B_n$-correctable;*
*(iii) there exists a sequence of $B_n$ and $P_n$ steps, such that after performing this sequence the resulting state $\rho'$ fulfils the inequality* $\mathrm{AsymCSS}(\rho') > 0$.

**Proof.** The equivalence of the first two statements was shown in corollary 1; that the second statement implies the third one is trivial, and that the third one implies the first follows from theorem 2 and conjecture 1 via contraposition. □

### *5.3. Values of the maximum tolerable error rate*

Using the criterion derived in the previous sections, one can calculate the maximum tolerable error rate for the BB84 and the six-state protocol assuming the model considered there. In the case of the six-state protocol $b = c = d$ holds [5]; thus, one only has to consider the so-called Werner states. Using the notation

$$\mathrm{W}(F) := \left(F, \frac{1-F}{3}, \frac{1-F}{3}, \frac{1-F}{3}\right), \qquad \mathrm{BB84}(F) := \left(F, \frac{1-F}{2}, \frac{1-F}{2}, 0\right), \tag{30}$$

one calculates for the six-state protocol

$$\begin{aligned} r[\mathrm{W}(F)] > 2 \quad &\Leftrightarrow \quad F > (5 + 3\sqrt{5})/20 \approx 0.585\,410 \\ &\Leftrightarrow \quad B < 1/2 - 1/(2\sqrt{5}) \approx 27.6393\%. \end{aligned} \tag{31}$$

For the BB84 protocol one can in principle use similar reasoning as the one by Gottesman–Lo [5], but the statement that the BB84($F$) state is the worst case for fixed bit-error rate $B$ can be proved much easier now. As before, $B = P = b + d = c + d$ and thus $b = c$ hold; using a suitable parameter $\delta \in [0; B]$, one can rewrite the state as

$$\rho = (1 - 2B + \delta, B - \delta, B - \delta, \delta). \tag{32}$$

By (12) it follows that $f(\rho) = 2\delta^2 + (2 - 6B)\delta + (1/2 - 7B/2 + 5B^2)$ and derivation with respect to $\delta$ yields $4\delta^2 + (2 - 6B) \geqslant 0$, if $B \leqslant 33.\bar{3}\%$. Therefore, $f$ increases monotonically with respect to $\delta$ and the worst case possible is $\delta = 0$, i.e. the BB84 state defined above. In this case, it follows

$$\begin{aligned} r[\mathrm{BB84}(F)] > 2 \quad &\Leftrightarrow \quad F > 3/5 = 0.600\,000 \\ &\Leftrightarrow \quad B < 1/5 = 20.0000\%. \end{aligned} \tag{33}$$

These maximum tolerable error rates coincide exactly with those given by Chau [6].

## 6. Conclusions

We analysed general entanglement purification protocols which imply the security of any quantum key distribution protocol whose security analysis can be reduced to the purification of Bell-diagonal states. These entanglement purification protocols are supposed to consist of arbitrary sequences of basic steps involving classical one- and/or two-way communication between Alice and Bob until the Shannon bound guarantees a successful completion of the entanglement purification on the basis of an appropriate CSS encoding and classical one-way communication. As a main result a condition on asymptotic correctability of Bell-diagonal qubit-pair states was presented relating the success of such protocol to the magnitude of a characteristic exponent. Applying this theorem to entanglement purification protocols of the Gottesman–Lo type we demonstrated that in the cases of the BB84 and six-state quantum cryptographic protocols secret keys can be generated even without any phase-error correcting steps of the Gottesman–Lo type up to the already known bit-error rates of $1/5 = 20\%$ and $1/2 - 1/(2\sqrt{5}) \approx 27.6393\%$. Furthermore, numerical evidence was provided that also the inclusion of additional arbitrary sequences of phase-error correcting steps cannot improve on these particular bounds.

On the other hand, it is still an open problem whether there exist other ways of post-processing (or even pre-processing) which allow the BB84 and the six-state protocol to tolerate higher error rates up to 25% and $33.\bar{3}\%$, respectively. For entanglement-based protocols this has been known for a long time, but no reduction to prepare-and-measure schemes is known. Another interesting problem is whether an exponent such as $r_{\mathrm{sup}}$ also exists for protocols using higher-dimensional Hilbert spaces, i.e. qudits (see also [14]).

## Acknowledgments

This work was supported by the EU within the IP SECOQC. Informative discussions with A Khalique, N Lütkenhaus and G Nikolopoulos are acknowledged. K Ranade is supported by a graduate-student scholarship of the Technische Universität Darmstadt.

## Appendix A. Evolution using $B_n$ and $P_n$ steps

### *A.1. Evolution using $B_n$ steps*

On two possibly different states $\rho = (a, b, c, d) \in \mathcal{S}_{\mathrm{bd}}$ and $\sigma = (p, q, r, s) \in \mathcal{S}_{\mathrm{bd}}$ a $B_2$ step is applied. After measuring and discarding the second qubit pair, the reduced density matrix of the first pair reads

$$\rho' = \left(\frac{ap+bq}{N}, \frac{bp+aq}{N}, \frac{cr+ds}{N}, \frac{dr+cs}{N}\right), \tag{A.1}$$

where $N = (a+b)(p+q) + (c+d)(r+s)$ is the normalization constant.

The proof of formulae (5) will be done by induction similar to that in [6]. In a $B_n$ step the $B_2$ step is used $(n-1)$ times, where $\rho$ is the first pair and $\sigma$ is a new pair every time, i.e. $\rho = B_k[(a,b,c,d)]$ and $\sigma = (a,b,c,d)$. One notes that the case $n = 1$ is trivial and $n = 2$ is the starting point of the induction. One now assumes that formulae (5) are valid for a fixed $n \in \mathbb{N}$. By using (A.1) one calculates for $(a',b',c',d') := B_{n+1}[(a,b,c,d)]$

$$\begin{aligned} a' &= [(a+b)^{n+1} + (a-b)^{n+1}]/2N' \qquad & b' &= [(a+b)^{n+1} - (a-b)^{n+1}]/2N' \\ c' &= [(c+d)^{n+1} + (c-d)^{n+1}]/2N' \qquad & d' &= [(c+d)^{n+1} - (c-d)^{n+1}]/2N', \end{aligned} \tag{A.2}$$

where $N' = [(a+b)^{n+1} + (c+d)^{n+1}]$ is the new normalization constant.

### A.2. Evolution using $P_n$ steps

The evolution of a state by applying $P_n$ steps is more complicated than that by applying $B_n$ steps. An analytical expression can be given by listing all possible combinations of Bell states, calculating the resulting Bell state systematically (by phase majority and bit parity) and adding them up according to their probability; for $P_n[(a,b,c,d)]$ it follows:

$$\sum_{(A,B,C,D)\in X_n} M(A,B,C,D)(a^A b^B c^C d^D, a^B b^A c^D d^C, a^C b^D c^A d^B, a^D b^C c^B d^A). \tag{A.3}$$

Here, $M(A,B,C,D) := (A+B+C+D)!/(A!B!C!D!)$ is a multinomial coefficient and $X_n := \{(A,B,C,D) \in \mathbb{N}_0^4 | A+B+C+D = n, A+C > B+D, A+B \text{ odd}\}$.

## Appendix B. Remarks to some theorems

### B.1. Proof of lemma 1

The idea of lemma 1 is to determine the exponential evolution of $f_n(p)$ and to absorb it into the value of $z^n$. Therefore, the appropriate value is $z(p) = \lim_{n\to\infty} \sqrt[n]{f_n(p)}$. In particular, $z(1/2) = 1$ and $z(1) = 0$. For the remaining cases $p \in (1/2; 1)$, one uses only the last term in the expression for $f_{2n+1}(p)$, which leads to

$$f_{2n+1}(p) = \sum_{k=0}^{n} \binom{2n+1}{k} p^k (1-p)^{2n+1-k} \geqslant \binom{2n+1}{n} p^n (1-p)^{n+1}. \tag{B.1}$$

The Stirling formula [13] $n^n\,\mathrm{e}^{-n}\sqrt{2\pi n} \leqslant n! \leqslant n^n\,\mathrm{e}^{-n}\sqrt{2\pi n}\,\mathrm{e}^{1/12n}$ yields

$$\frac{n+1}{2n+1} \cdot \binom{2n+1}{n} = \frac{(2n)!}{(n!)^2} \geqslant \frac{(2n)^{2n}\,\mathrm{e}^{-2n}\sqrt{2\pi(2n)}}{n^{2n}\,\mathrm{e}^{-2n} 2\pi n\,\mathrm{e}^{1/6n}} = 2^{2n}\frac{\mathrm{e}^{-1/6n}}{\sqrt{\pi n}}. \tag{B.2}$$

Thus, $\binom{2n+1}{n} \geqslant 2^{2n+1} h(n)$ with $h(n) = \mathrm{e}^{-1/6n}\left(1 - \frac{1}{2(n+1)}\right)\big/\sqrt{\pi n}$ and therefore

$$f_{2n+1}(p)^{\frac{1}{2n+1}} \geqslant 2h(n)^{\frac{1}{2n+1}} p^{\frac{1}{2+\frac{1}{n}}} (1-p)^{\frac{1}{2-\frac{1}{n+1}}} \overset{n\to\infty}{\longrightarrow} 2\sqrt{p(1-p)}. \tag{B.3}$$

By this $z(p) \geqslant 2\sqrt{p(1-p)}$ was proved. The inequality $z(p) \leqslant 2\sqrt{p(1-p)}$ is a special case of the Chernoff bound (cf [12], p 154, (3.5)).

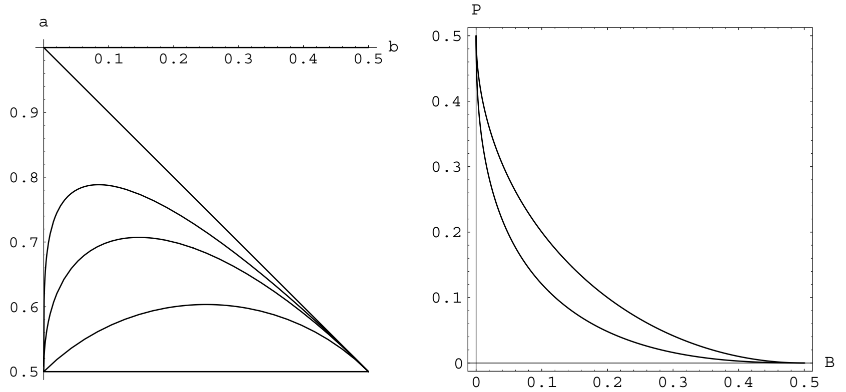


**Figure B1.** Left: minimum fidelity for $r > 2$, $r_P > 1$ and $r_P > 2$ (bottom to top); right: lines for AsymCSS$(B, P) = 0$ and $r_P = 1$.

### *B.2. Proof of theorem 2*

*B.2.1. On the first implication* (AsymCSS$(\rho) > 0 \Rightarrow r_P > 1$). For the proof of the first implication, one notes that AsymCSS and $r_P$ can be considered as functions of $B$ and $P$ and that AsymCSS$(B_1, P_1) \geqslant$ AsymCSS$(B_2, P_2)$ holds if $0 \leqslant B_1 \leqslant B_2 \leqslant 1/2$ and $0 \leqslant P_1 \leqslant P_2 \leqslant 1/2$. Because of (18) it has to be shown that AsymCSS$(B, P) \leqslant 0$ is true on the circular arc defined by $r_P = 1$ (see figure B1), i.e. that

$$h(t) := 1 - H[(\cos t)/2] - H[(\sin t)/2] \leqslant 0 \tag{B.4}$$

is valid for $t \in [0; \pi/2]$; by symmetry of the function, it is sufficient to show the property for $t \in [0; \pi/4]$. Using $h(0) = 0$, it is further sufficient to show that $h'(t) \leqslant 0$ for $\in [0; \pi/4]$, i.e.

$$(\ln 4 \cdot h')(t) = \cos t[\ln \sin t - \ln(2 - \sin t)] - \sin t[\ln \cos t - \ln(2 - \cos t)] \leqslant 0. \tag{B.5}$$

Rewriting this inequality yields $\sin t[\ln(2 - \cos t) - \ln \cos t] \leqslant \cos t[\ln(2 - \sin t) - \ln \sin t]$ and because $t \in [0; \pi/4]$ implies $\cos t \geqslant \sin t \geqslant 0$, it further only remains to show that

$$h'_B(t) := \ln(2 - \cos t) - \ln \cos t - \ln(2 - \sin t) + \ln \sin t \leqslant 0 \tag{B.6}$$

is valid. By $h''_B(t) = (\sin t/(2 - \cos t)) + \tan t + (\cos t/(2 - \sin t)) + \cot t$, $h''_B(t) \geqslant 0$ for $t \in [0; \pi/4]$, and thus, $h'_B$ increases monotonically. Finally, $h'_B(\pi/4) = 0$, which implies the assertion.

*B.2.2. On the second implication* ($r_P > 1 \Rightarrow r > 2$). The proof of the second implication can also be visualized by figure B1. Plotting the minimum fidelity $a \in [1/2; 1]$, for which $r > 2$ is true, as a function of $b \in [0; 1/2]$ results in the function

$$f_{r=2}(b) := 1/4 + \sqrt{1/8 - (b - 1/4)^2}. \tag{B.7}$$

Because $r_P$ depends upon the error rates $B$ and $P$, it is not directly possible to plot the minimum fidelity $a$ as a function of $b$. Assuming the best case (i.e. the smallest minimum fidelity possible), one assumes the minimum phase-error rate and therefore $d = 0$. In this case the limiting function is

$$f_{r_P=1}(b) := 1 - b - (1/2 - \sqrt{b(1 - b)}). \tag{B.8}$$

For proving $f_{r_P=1} \geqslant f_{r=2}$ (see also figure B1), let $\Delta(b) := f_{r_P=1}(b) - f_{r=2}(b)$. It has to be shown that $\Delta(b) \geqslant 0$ for $b \in [0; 1/2]$. This function is continuous and by the intermediate value theorem, it is sufficient to show that $b_1 = 0$ and $b_2 = 1/2$ are the only points where it is zero and that there exists a point $b$ where $\Delta(b) > 0$. Repeated squaring of the equation $\Delta(b) = 0$ yields a necessary condition for any zero of $\Delta$:

$$5b^4 - 6b^3 + 9b^2/4 - b/4 = 5b(b - 1/5)(b - 1/2)^2 = 0. \tag{B.9}$$

The set of zeros of the last equation is $\{0, 1/5, 1/2\}$. Because of $\Delta(0) = \Delta(1/2) = 0$ and $\Delta(1/5) = 1/10 > 0$, $\Delta$ is non-negative on the whole interval $[0; 1/2]$.

### *B.3. Remarks to conjecture 1*

Some details regarding lemmata 4 and 5 are given. Before continuing, note the following lemma (the proof is trivial):

**Lemma 6** (Monotonicity of the binomial distribution). *Let $n \in \mathbb{N}_0$ and $r \in \{0, \ldots, n\}$. The function $f : [0; 1] \to [0; 1]$, which is defined by $f(x) := \sum_{k=0}^{r} \binom{n}{k} x^k (1 - x)^{n-k}$ decreases monotonically in x.*

*B.3.1. On the first reduction.* It remains to show that $a'$ is maximal if $z = 1$. By (A.3) it follows using $\rho = Z(a, b; z)$ and $K := C + D$ and $(A, B, C, D) \in X_n$ that $a' = \sum_{A,B} M(A, B, C + D, 0) a^A b^B (1 - a - b)^{C+D} \sum_{D=0}^{D_{\max}} \binom{K}{D} z^{K-D} (1 - z)^D$. For $a'$ being maximal, it is sufficient that for all possible $A, B, K$ each term of the inner sum becomes maximal. For fixed $A$ and $B$ the sum over $D$ is of such a form, that lemma 6 can be applied, i.e. $a'$ becomes maximal when $(1 - z) = 0$ or $z = 1$ hold.

*B.3.2. On the second reduction.* The proof is similar to the previous one. Using $K := A + B$ yields $a' = \sum_C \binom{n}{C} c^C \sum_{B=0}^{B_{\max}} \binom{K}{B} (a - \varepsilon)^{K-B} (b + \varepsilon)^B$. As before the maximality of the inner sum is sufficient for the maximality of $a'$. If one divides this by $(a + b)^K$, the assertion follows by lemma 6.

## References


[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Computers on Systems and Signal Processing* (Bangalore: India) 175
[2] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[3] Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098
[4] Steane A M 1996 *Proc. R. Soc. London* A **452** 2551
[5] Gottesman D and Lo H K 2003 *IEEE Trans. Inf. Theor.* **49** 457
[6] Chau H F 2002 *Phys. Rev.* A **66** 060302
[7] Bruss D 1998 *Phys. Rev. Lett.* **81** 3018
[8] Ranade K S 2005 Quantenkryptographie und Verschränkung *Diploma Thesis* (TU Darmstadt: Germany)
[9] Bennett C H, DiVicenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824
[10] Lo H K and Chau H F 1999 *Science* **283** 2050
[11] Wang X B 2004 Criteria for unconditional entanglement purification *Preprint* quant-ph/0403058
[12] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[13] Abramowitz M and Stegun I A 1965 *Handbook of Mathematical Functions* (New York: Dover)
[14] Nikolopulos G M, Ranade K S and Alber G 2005 (submitted to *Phys. Rev. A*)