Augmented message-matrix approach to deterministic dense-coding theory

E. Gerjuoy*
Department of Physics, University of Pittsburgh, Pittsburgh, Pennsylvania 15260, USA

H. T. Williams†
Department of Physics and Engineering, Washington and Lee University, Lexington, Virginia 24450, USA

P. S. Bourdon‡
Department of Mathematics, Washington and Lee University, Lexington, Virginia 24450, USA

(Received 4 September 2008; published 13 April 2009)

A useful method for deriving analytical results applicable to the standard two-party deterministic dense-coding protocol is introduced and illustrated. In this protocol, communication of K perfectly distinguishable messages is attainable via K selected local unitary operations performed on one qudit from a pair of entangled qudits of equal dimension d in a pure state $|\psi\rangle$ with largest Schmidt coefficient $\sqrt{\lambda_0}$. The method takes advantage of the fact that the K message states, together with d^2-K augmenting orthonormal state vectors, yield a unitary matrix, thereby implying properties of the K message states which otherwise are not readily recognized. Employing this augmented message matrix, we produce simple proofs of previously established results including (i) $\lambda_0 \leq d/K$, (ii) $\lambda_0 < d/K$ when $K=d+1$, and (iii) the impossibility of finding a $|\psi\rangle$ that can enable transmission of $K=d^2-1$ messages but not d^2. Additional results obtained using the method include proofs that the $\lambda_0 \leq d/K$ bound is reduced to at least (i) $\lambda_0 \leq (1/2)[1+\sqrt{(d-2)/(d+2)}]$ when $K=d+1$ and (ii) $\lambda_0 \leq (K-m)/(2K-m-d)$ whenever $(d+1) \leq K \leq 2d$ and the selected local unitaries include the first m non-negative integral powers of the shift operator X.

DOI: 10.1103/PhysRevA.79.042315 PACS number(s): 03.67.Hk, 03.65.Ud

I. INTRODUCTION AND FORMALISM

The deterministic dense-coding protocol first described by Bennett and Wiesner [1] in 1992 has been the subject of numerous investigations ([2–6] and references therein). Here, therefore, we describe the protocol and its associated formalism only briefly.

Alice and Bob, who are located far apart, each controls one qudit from an entangled pair. Orthonormal basis sets for Alice's and Bob's qudits, in their respective Hilbert spaces H_A and H_B, are denoted, respectively, by $|i\rangle_A$ and $|j\rangle_B$, $i,j=0,1,\ldots,(d-1)$. Initially the pair of qudits is in a normalized entangled pure state $|\psi\rangle$, with Schmidt representation

$$|\psi\rangle = \sum_{j=0}^{d-1} \sqrt{\lambda_j}|j\rangle_A|j\rangle_B \equiv \sum_{j=0}^{d-1} \sqrt{\lambda_j}|jj\rangle. \tag{1.1}$$

In Eq. (1.1) the Schmidt coefficients $\sqrt{\lambda_j}$ are non-negative real numbers satisfying $\Sigma_{j=0}^{d-1}\lambda_j=1$; we make the conventional assumption without loss of generality that $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{d-1} \geq 0$. The right side of Eq. (1.1) makes use of the convenient notation, which we shall employ henceforth, that $|ij\rangle$ denotes the product basis state $|i\rangle_A|j\rangle_B$; collectively these states form a complete orthonormal basis set in the d^2-dimensional Hilbert space $H=H_A \otimes H_B$, wherein lie $|\psi\rangle$ and all other state functions describing the state of the qudit pair. Alice performs a local unitary operation U_A on her qudit and then sends the qudit to Bob via a noise-free quantum channel. Any such U_A converts $|\psi\rangle$ to the normalized state function,

$$|\Psi\rangle = (U_A \otimes I_B)|\psi\rangle = \sum_{i,j=0}^{d-1} \sqrt{\lambda_j}U_{ij}|ij\rangle, \tag{1.2}$$

where U_{ij} denotes the matrix element $\langle i|U_A|j\rangle$ of the operator $U_A=\Sigma_{i,j=0}^{d-1}U_{ij}|i\rangle_A\langle j|_A$. Let $\{U^{(a)}\}_{a=0}^{K-1}$ be a set of K local unitaries having the special property that the K corresponding $|\Psi^{(a)}\rangle$'s are mutually orthogonal, with K here and hereinafter the largest possible number of such unitaries for a given $|\psi\rangle$. As Mozes *et al.* [2] observed, the condition that the $U^{(a)}$ constitute such a set is expressed by the requirement that for every a,b pair in the set,

$$\langle\Psi^{(a)}|\Psi^{(b)}\rangle \equiv \sum_{i,j=0}^{d-1} \lambda_j (U_{ij}^{(a)})^* U_{ij}^{(b)} = \mathrm{tr}[\Lambda (U^{(a)})^\dagger U^{(b)}] = \delta_{ab}, \tag{1.3}$$

where $\langle\Psi^{(a)}|\Psi^{(b)}\rangle$ denotes the Hilbert-space H scalar product of $|\Psi^{(a)}\rangle$ and $|\Psi^{(b)}\rangle$, and Λ is a diagonal $d\times d$ matrix whose diagonal elements are the squares of the Schmidt coefficients defined in Eq. (1.1), i.e., $\Lambda_{ij}=\lambda_i\delta_{ij}$. A set $\{U^{(a)}\}$ satisfying Eq. (1.3) will be termed "Λ orthogonal."

If Bob knows Alice has operated on $|\psi\rangle$ with one of the K unitaries in some given Λ-orthogonal set $\{U^{(a)}\}$, then Bob—after receiving Alice's qudit—can correctly determine which particular $U^{(a)}$ Alice actually employed before sending her qudit. Thus this protocol enables Alice to send Bob one of K previously agreed-upon possible messages. Deterministic dense-coding theory seeks to answer the question: given

*gerjuoy@pitt.edu
†williamsh@wlu.edu
‡pbourdon@wlu.edu

specified values for the Schmidt coefficients, what is the corresponding value of K? It has been demonstrated [1] that when every $\lambda_i = 1/d$ in Eq. (1.1), i.e., when $|\psi\rangle$ is maximally entangled, then $K = d^2$. For nonmaximally entangled $|\psi\rangle$, however, tantalizing open questions remain about the dependence of K on the λ_i, despite significant scrutiny given to the dense-coding theory. In particular, Mozes *et al.* [2] numerically explored this dependence in great detail for the three-dimensional case ($d=3$), and in lesser but still illuminating detail for $d=4$ to 7. In so doing, they produced several interesting conjectures which will be examined among the issues treated herein.

A. Results

Given any set of K unitaries $\{U^{(a)}\}_{a=0}^{K-1}$ constituting a Λ-orthogonal set, Eq. (1.3) shows the corresponding $\{\Psi^{(a)}\}_{a=0}^{K-1}$ can be thought of as a set of K orthonormal basis vectors for a K-dimensional subspace S_K of the d^2-dimensional Hilbert space H. Any set of d^2-K orthonormal basis vectors $\{\Phi^{(b)}\}_{b=K}^{d^2-1}$ contained in the subspace $S_{d^2\text{-}K}$ orthocomplementary to S_K must be orthogonal to the set $\{\Psi^{(a)}\}_{a=0}^{K-1}$. Thus the $\{\Psi^{(a)}\}_{a=0}^{K-1}$ taken together with the $\{\Phi^{(b)}\}_{b=K}^{d^2-1}$ constitute an orthonormal basis for H. Of course, both the $|\Psi^{(a)}\rangle$ and the $|\Phi^{(b)}\rangle$ can be expressed in terms of their components along elements of the previously defined basis $\{|ij\rangle : 0 \le i,j \le d-1\}$,

$$|\Psi^{(a)}\rangle = \sum_{i,j=0}^{d-1} \sqrt{\lambda_j} U_{ij}^{(a)} |ij\rangle, \quad |\Phi^{(b)}\rangle = \sum_{i,j=0}^{d-1} \phi_{ij}^{(b)} |ij\rangle. \tag{1.4}$$

It is convenient to order the basis of H in a nonstandard way as follows:

$$\begin{aligned}&(|00\rangle, |10\rangle, \ldots, |(d-1)0\rangle, |01\rangle, |11\rangle, \ldots, |(d-1)1\rangle, \\ &\ldots, |0(d-1)\rangle, |1(d-1)\rangle, \ldots, |(d-1)(d-1)\rangle).\end{aligned} \tag{1.5}$$

Henceforth this ordering of the $|ij\rangle$ and the corresponding ordering of components of each $|\Psi^{(a)}\rangle$ and $|\Phi^{(b)}\rangle$ will be employed herein.

Central to our approach is the $d^2 \times d^2$ matrix M, whose entries are the components, appearing in Eq. (1.4), of the vectors $|\Psi^{(a)}\rangle$ and $|\Phi^{(b)}\rangle$. For $0 \le a \le K-1$, column a of M comprises the components of $|\Psi^{(a)}\rangle$; for $K \le b \le d^2-1$, column b of M comprises the components of $|\Phi^{(b)}\rangle$. Accordingly, we call M an *augmented message-matrix* because it is composed of the column vectors representing the two-qudit states $|\Psi^{(a)}\rangle$ that Alice can prepare as messages for Bob augmented with enough additional vectors (those representing $|\Phi^{(b)}\rangle$) to form a $d^2 \times d^2$ matrix. The aforesaid ordering means that in any given row of M, the entry in each column is the component (of the corresponding $|\Psi^{(a)}\rangle$ or $|\Phi^{(b)}\rangle$) along the same uniquely specified $|ij\rangle$; therefore the d^2 rows of M can be labeled by ij pairs, where $i,j = 0,1,\ldots,(d-1)$. Our ordering further implies [recall Eq. (1.5)] that if we count the d^2 rows starting from the top row as 0, so that the last (and bottom) row is row d^2-1 then the row labeled by ij actually is row $jd+i$. It follows that row $jd+i$ has the entries

$$M_{ij,a} = \sqrt{\lambda_j} U_{ij}^{(a)} \text{ for } a = 0, \ldots, K-1,$$
$$M_{ij,b} = \phi_{ij}^{(b)} \text{ for } b = K, \ldots, d^2-1.$$

Because the columns of M are composed of the components of the orthonormal-basis vectors $|\Psi^{(a)}\rangle$, $|\Phi^{(b)}\rangle$, the matrix M must be unitary. The unitarity of M provides inherent restrictions on components of the K message states $|\Psi^{(a)}\rangle$ that have not been recognized before. In particular, the rows of M also constitute an orthonormal set and hence necessarily satisfy

$$\begin{aligned}&\sum_{a=0}^{K-1} M_{ij,a}(M_{i'j',a})^* + \sum_{b=K}^{d^2-1} M_{ij,b}(M_{i'j',b})^* \\ &\equiv \sqrt{\lambda_j \lambda_{j'}} \sum_{a=0}^{K-1} U_{ij}^{(a)}(U_{i'j'}^{(a)})^* + \sum_{b=K}^{d^2-1} \phi_{ij}^{(b)}(\phi_{i'j'}^{(b)})^* = \delta_{i,i'}\delta_{j,j'}.\end{aligned} \tag{1.6}$$

Equation (1.6) is the key relationship of our augmented message-matrix approach. It leads to surprisingly simple derivations of previously proved dense-coding results, as well as of new restrictions on the possible values of K as a function of the Schmidt coefficients of $|\psi\rangle$.

By way of illustration, we present an especially simple proof of an important prior result. Treating rows of the augmented message-matrix as vectors, each is of squared length 1,

$$\lambda_j \sum_{a=0}^{K-1} |U_{ij}^{(a)}|^2 + \sum_{b=K}^{d^2-1} |\phi_{ij}^{(b)}|^2 = 1.$$

For fixed j, sum both sides of the preceding equation from $i=0$ to $d-1$ and utilize the unitarity of the $U^{(a)}$'s to obtain

$$K\lambda_j + \sum_{b=K}^{d^2-1} \sum_{i=0}^{d-1} |\phi_{ij}^{(b)}|^2 = d, \tag{1.7}$$

leading immediately for the case $j=0$ to

$$\lambda_0 \le d/K.$$

This upper bound on the value of λ_0 permitting K unitaries that are Λ orthogonal, originally conjectured by Mozes *et al.* [2], was first deduced by Wu, Cohen, Sun, and Griffiths (WCSG) [4] employing density-matrix manipulations. Subsequently Bourdon *et al.* [6] produced a derivation of this bound, which we will refer to as the WCSG bound, that avoided the introduction of density matrices, instead utilizing projection operator techniques.

Additional results we have achieved using our augmented-matrix approach are described and placed in context in the following:

(i) The numerical analysis of Mozes *et al.* [2] indicates that when $K=d+1$, the WCSG bound $\lambda_0 \le d/(d+1)$ overestimates the permitted values of λ_0. Bourdon *et al.* [6] (Proposition II.3) established that when $K=d+1$ the WCSG bound indeed is unsaturated, i.e., that in this circumstance $\lambda_0 = d/(d+1)$ cannot hold. In Sec. II we present a shorter and simpler augmented message-matrix proof of this nonsaturation result. Moreover, as Sec. II shows, this proof immediately generalizes to a demonstration that the WCSG bound for $K=md+1$ is not saturated when $1\leq m\leq d$ and the m largest Schmidt coefficients of $|\psi\rangle$ are equal, which is a recent result of Beran and Cohen [7] originally obtained via a much longer proof relying on Gersgorin's theorem on the locations of matrix eigenvalues.

(ii) Based primarily on numerical evidence, Mozes *et al.* conjectured that there is no set of Schmidt coefficients that allow $K=d^2-1$; i.e., they conjectured that whenever the state $|\psi\rangle$ of a two-qudit system supports the transmission of d^2-1 messages via dense coding then $|\psi\rangle$ is maximally entangled (and therefore $K=d^2$). They proved this result analytically for $d=2$ only. Ji *et al.* [3] settled this conjecture for all d, utilizing partial trace techniques and the concavity of the von Neumann entropy of the entangled states. Section III presents a simple proof for all d, utilizing straightforward manipulation of Eq. (1.6).

(iii) The numerical analysis of Mozes *et al.* strongly suggested that when $K=d+1$, the WCSG bound quoted in the first paragraph (i) above must be replaced by the much more restrictive $\lambda_0\leq(d-1)/d$. In Sec. IV we prove the result that when $K=d+1$, the WCSG bound reduces to at least $\lambda_0\leq(1/2)[1+\sqrt{(d-2)/(d+2)}]\equiv r$, where it is easily seen that for $d>2$ the bound r satisfies $(d-1)/d<r<d/(d+1)$.

(iv) By explicitly constructing $d+1$ Λ-orthogonal unitaries, two of which were the identity I and the shift operator X (defined in Sec. V below), Mozes *et al.* showed that there is a state $|\psi\rangle$, with $\lambda_0=(d-1)/d$ and $\lambda_2=0$ in Eq. (1.1), for which K can equal $d+1$. When $K=d+1$, therefore, the WCSG bound on λ_0 cannot be reduced below $(d-1)/d$. Whether there exists any Eq. (1.1) $|\psi\rangle$ permitting $K=d+1$ with $(d-1)/d<\lambda_0\leq r$ (where r is defined immediately above) remains an open question, although the numerical results of Mozes *et al.* strongly suggested this not to be the case. In Sec. V we show, as has not been previously shown, that whenever one has a family of $d+1$ Λ-orthogonal unitaries, two of which are I and X, then the WCSG bound does reduce all the way to $(d-1)/d$. In other words, we have shown that if there exists a family of $d+1$ Λ-orthogonal unitaries for any $\lambda_0>(d-1)/d$, that family cannot contain both I and X. Note (see, e.g., the proof of Lemma II.1 in [6]) that one always can assume, without loss of generality insofar as restrictions on λ_0 are concerned, that a family of Λ-orthogonal unitaries includes either I or X.

(v) Bounds which can improve on the WCSG bound even when $K>d+1$ also are derived in Sec. V; these improved bounds stem from previously unrecognized generalizations of some of the results described in the preceding paragraph. In particular, we show that $\lambda_0\leq(K-m)/(2K-m-d)\equiv s$ whenever $(d+1)\leq K\leq 2d$ and the selected local unitaries include the first m non-negative integer powers of the shift operator X. For $m=1$ this bound never offers any improvement on the WCSG bound. For $m>1$, however, s can lie well below the WCSG bound; when $d=4$, $K=6$, $m=3$, for example, $s=3/5$, whereas the WCSG bound is 4/6.

II. NONSATURATION PROOFS

We will employ our augmented message-matrix approach to prove the WCSG bound $\lambda_0\leq d/K$ always is unsaturated when $K=d+1$. Assume, in order to obtain a contradiction, that λ_0 does equal $d/(d+1)$, i.e., that $\lambda_0K=d$. Then, returning to our proof of the WCSG bound in Sec. I A, we see that Eq. (1.7), with $j=0$, immediately implies that $\phi_{i0}^{(b)}=0$ for every $i=0,\ldots,d-1$ and $b=d+1,\ldots,d^2-1$. In other words, each ϕ column of the augmented message matrix M consists of zeros through entry $i=d-1$, $j=0$. Thus the remaining entries in the $\phi^{(b)}$ vectors comprise an orthonormal collection of d^2-d-1 vectors in $\mathbb{C}^{d^2-d}$. Let W be the span of these vectors so that W is a d^2-d-1 dimensional subspace of $\mathbb{C}^{d^2-d}$. The orthocomplement $W^{\perp}$ of W is thus one dimensional; let v be a unit vector spanning $W^{\perp}$. For any $a\in\{0,1,\ldots,d\}$, let $v^{(a)}$ be the necessarily nonzero vector (since $\lambda_0<1$ implies $\lambda_1>0$) in $\mathbb{C}^{d^2-d}$ formed by the 0 1 through $(d-1)(d-1)$ entries of column a of M. Orthogonality of columns of M implies that $v^{(a)}$ belongs to $W^{\perp}$ for each a, so that there are nonzero constants β_a such that $v^{(a)}=\beta_a v$ for each $a\in\{0,1,\ldots,d\}$. Thus for each $a\in\{1,2,\ldots,d\}$, there is a nonzero constant γ_a such that

$$v^{(a)}=\gamma_a v^{(0)}. \tag{2.1}$$

Observe that both $v^{(a)}$ and $v^{(0)}$ have length $1-\lambda_0$ so that $|\gamma_a|=1$. Rewriting Eq. (2.1), we have

$$\sqrt{\lambda_j}U_{ij}^{a}=\gamma_a\sqrt{\lambda_j}U_{ij}^{0}$$

for $j=1,\ldots,d-1$, $i=0,\ldots,d-1$, and $a=1,\ldots,d$. Because $U^{(0)}=I$ and $\lambda_1\neq 0$, we see from the preceding equation that for each $a\in\{1,\ldots,d\}$, the column of $U^{(a)}$ with elements $U_{i1}^{(a)}$ is the unimodular constant γ_a times the same column of I, with elements δ_{i1}. Hence, because $U^{(a)}$ is unitary, its row with elements $U_{1j}^{(a)}$ is all zeros but for the $j=1$ element. It follows that the row of M with elements $M_{10,a}$ has zeros for entries $a=0$ through $a=d$; but the remaining entries, the "ϕ" entries, are also zero, contradicting the fact that M is unitary. This contradiction leads us to conclude that for $K=d+1$, λ_0 must satisfy the strict inequality relationship

$$\lambda_0<\frac{d}{d+1}.$$

The preceding proof immediately generalizes to yield the result by Beran and Cohen [7] mentioned in paragraph (i) of Sec. I A. Suppose now that $K=md+1$ and that $\lambda_0=\lambda_1=\ldots=\lambda_{m-1}$, where $1\leq m<d$. We will show the WCSG bound $\lambda_0\leq d/K$ also is unsaturated in this circumstance, i.e., that here λ_0 must be $<d/(md+1)$. Again assume, in order to obtain a contradiction that $\lambda_0=d/(md+1)=d/K$. Then, just as in the preceding proof, Eq. (1.7) implies $\phi_{ij}^{(b)}=0$ for $i=0,\ldots,d-1$, $j=0,\ldots,m-1$, and $b=md+1,\ldots,d^2-1$. Thus we can conclude that under our present assumptions, each $\phi^{(b)}$ column of M consists of zeros from the first $|00\rangle$ row through the $|d-1,m-1\rangle$ row, i.e., through the first md rows.

Thus, in complete analogy with the previous proof, the remaining entries in the $\phi^{(b)}$ columns constitute an orthonormal collection of d^2-md-1 vectors in $\mathbf{C}^{d^2-md}$, and the subspace spanned by $\{v^{(a)}\}_{a=0}^{md}$ is one dimensional, where $v^{(a)}$ is the vector formed by the md through d^2-1 entries of column a of M. This vector is necessarily nonzero, since $\lambda_0+\lambda_1+\ldots+\lambda_{m-1}=m\lambda_0=md/(md+1)<1$, implying $\lambda_m>0$. Then, still proceeding as in the previous proof, we readily further conclude that for each $a \in \{1,\ldots,md\}$ and every $i=0,\ldots,d-1$,

$$U_{im}^{(a)} = \gamma_a U_{im}^{(0)} = \gamma_a \delta_{im},$$

where γ_a is a unimodular constant. It follows, again as before, that the row of M with elements $M_{m0,a}$ has zeros for entries $a=0$ through $a=md$. But in the immediately preceding paragraph, the remaining entries in this row of M—the $\phi^{(b)}$ entries—also have been shown to equal zero. Once again, therefore, we have established a contradiction with the fundamental principle that M is unitary, thereby demonstrating that the set of Schmidt coefficients with $\lambda_0=\lambda_1=\ldots=\lambda_{m-1}$, where $1\le m<d$, cannot support $K=md+1$ Λ-orthogonal unitaries, i.e., that in this circumstance the WCSG bound necessarily is unsaturated.

III. IMPOSSIBILITY OF ONLY d^2-1 ENCODING UNITARIES IN d DIMENSIONS

It is known that under the d-dimensional deterministic dense-coding protocol, there is a region of the space of the λ_j that admits a maximum of $K=d$ encoding unitaries (coinciding with the limit of classical communication) as well as a second region (actually no more than a point) wherein one can find as many as $K=d^2$ encoding unitaries, the maximum number possible in view of the fact that our initial $|\psi\rangle$ of Eq. (1.1) lies in a d^2-dimensional Hilbert space. One expects, therefore, that there should be regions of the λ_j space wherein $K=m$ but no more than m encoding unitaries can be found, for every integer value of m from $m=d+1$ to $m=d^2-1$. One of the more counterintuitive properties of the protocol is that this just-stated expectation is met for every such m except $m=d^2-1$. The only point in the space of λ_j's that allows d^2-1 encoding unitaries also allows d^2, occurring at the point where $\lambda_j=1/d$ for all j. This result was proven by Ji *et al.* [3], using the spectral properties of partial traces of density operators and the concavity of the von Neumann entropy. Our approach allows this result to be established algebraically from the unitarity properties of the encoding $U^{(a)}$'s and the corresponding augmented message matrix M introduced in Sec. I.

Consider the d-dimensional situation, with $K=d^2-1$ encoding unitaries $\{U^{(a)}\}_{a=0}^{d^2-2}$. From the WCSG bound discussed in Sec. I A, we know in this case $\lambda_0\le d/(d^2-1)$, and it is easily seen that this ensures that all the λ_i are nonzero. The sum over a in Eq. (1.6) involves d^2-1 terms, and the sum over b has only a single term allowing us to drop the superscript $b=d^2-1$ on ϕ for this case. Extract from Eq. (1.6) the following relationship by setting $j'=j$, dividing through by λ_j, and summing the result over j:

$$\delta_{ii'}\sum_{j=0}^{d-1}\frac{1}{\lambda_j} = \sum_{a=0}^{d^2-2}\sum_{j=0}^{d-1} U_{ij}^{(a)}(U_{i'j}^{(a)})^* + \sum_{j=0}^{d-1}\frac{\phi_{ij}\phi_{i'j}^*}{\lambda_j}.$$

Since each of the d^2-1 $U^{(a)}$'s is unitary, we reach

$$\sum_{j=0}^{d-1}\frac{\phi_{ij}\phi_{i'j}^*}{\lambda_j} = \left[\sum_{j=0}^{d-1}\frac{1}{\lambda_j} - (d^2-1)\right]\delta_{ii'}. \tag{3.1}$$

This equation can be interpreted as describing the properties of a $d\times d$ matrix S, with its i,j element equal to $\phi_{ij}/\sqrt{\lambda_j}$, whose rows (labeled by $0\le i\le d-1$) are vectors which are mutually orthogonal, and each of which has a common length, the square of which may be computed by setting $i'=i$ in Eq. (3.1),

$$\sum_{j=0}^{d-1}\frac{|\phi_{ij}|^2}{\lambda_j} = \sum_{k=0}^{d-1}\frac{1}{\lambda_k} - (d^2-1).$$

Note that the value of the common row lengths must be nonzero; otherwise all components ϕ_{ij} of the unit vector ϕ would be zero: a contradiction. Such a matrix, within a constant multiple of a unitary matrix, will have its columns (labeled by $0\le j\le d-1$) representable as vectors with the same lengths as the row vectors; thus

$$\sum_{i=0}^{d-1}\frac{|\phi_{ij}|^2}{\lambda_j} = \sum_{k=0}^{d-1}\frac{1}{\lambda_k} - (d^2-1). \tag{3.2}$$

From Eq. (1.7) we arrive at another expression for the squares of these lengths (recalling we have dropped the superscript $b=d^2-1$ on ϕ),

$$\sum_{i=0}^{d-1}\frac{|\phi_{ij}|^2}{\lambda_j} = \frac{d}{\lambda_j} - (d^2-1). \tag{3.3}$$

In combination, Eqs. (3.2) and (3.3) produce

$$\sum_{k=0}^{d-1}\frac{1}{\lambda_k} = \frac{d}{\lambda_j},$$

true for each j, $0\le j\le d-1$. This is only possible if all the λ_j's are equal, and since they sum to one, necessarily $\lambda_j=1/d$ for each j. This corresponds to the set of Schmidt coefficients for maximal entanglement, the point at which d^2 encoding unitaries can be found. Thus we have proved that if we can find d^2-1 encoding unitaries, we must be able to find d^2, i.e., there is no region in the space of the λ_j that admits a maximum of $K=d^2-1$ encoding unitaries.

Evaluating the expression for the common length of the row and column vectors of the matrix S,

$$\sum_{k=0}^{d-1}\frac{1}{\lambda_k} - (d^2-1) = \sum_{k=0}^{d-1} d - (d^2-1) = 1,$$

and because (as previously noted) the rows of S are orthogonal, this shows S to be unitary, and—in fact—to be the last encoding unitary matrix,

$$U_{ij}^{(d^2-1)} = S_{ij} = \frac{\phi_{ij}}{\sqrt{\lambda_j}}.$$

IV. BOUND FOR THE $K=d+1$ CASE

The WCSG bound for the case $K=d+1$ is $\lambda_0\le d/(d+1)$. A smaller bound $\lambda_0\le(d-1)/d$ was conjectured by Mozes *et* *al.* [2] based on the failure of a numerical-search procedure to find families of $d+1$ encoding unitaries when the value of λ_0 exceeds $(d-1)/d$. Also providing some support of their conjecture, Mozes *et al.*, for all d, analytically constructed families of $d+1$ encoding unitaries for $\lambda_0=(d-1)/d$ and $\lambda_j=0$ for $j\geq 2$. Using the augmented message matrix, we establish here an upper bound on λ_0 for the case $K=d+1$ that is a finite distance below the WCSG bound of $d/(d+1)$ but not as small as the conjectured bound $(d-1)/d$. Throughout this section, we assume that λ_0 is confined to the region of interest: $(d-1)/d\leq\lambda_0\leq d/(d+1)$. We focus our attention on dimensions d higher than two, the one case in which the conjectured bound has been proven. Thus, in particular, if λ_0 lies in our region of interest then $\lambda_0>1/2$.

Assume that Alice can create a maximum of $K=d+1$ distinguishable messages. We assume $U^{(0)}$ to be the identity operator, so that the entries in the first column of the augmented message matrix M are

$$M_{ij,0}=\sqrt{\lambda_j}U_{ij}^{(0)}=\sqrt{\lambda_j}\delta_{ij}.$$

Λ orthogonality of each $U^{(a)}$, $1\leq a\leq d$, with $U^{(0)}$, which is equivalent to the orthogonality of columns a and 0 of M, leads to

$$\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}M_{ij,a}M_{ij,0}^{*}=\sum_{i=0}^{d-1}\lambda_i U_{ii}^{(a)}=0. \qquad (4.1)$$

Define real constants $\eta_i\equiv\lambda_i/\lambda_0$ for $1\leq i\leq d-1$ and use them to write

$$|U_{00}^{(a)}|=\left|\sum_{i=1}^{d-1}\eta_i U_{ii}^{(a)}\right|\leq\sum_{i=1}^{d-1}\eta_i|U_{ii}^{(a)}|,\quad 1\leq a\leq d,$$

where the final step follows from the triangle inequality. From this it follows simply that

$$\sum_{a=0}^{d}|U_{00}^{(a)}|^2=1+\sum_{a=1}^{d}|U_{00}^{(a)}|^2\leq 1+\sum_{a=1}^{d}\left(\sum_{i=1}^{d-1}\eta_i|U_{ii}^{(a)}|\right)^2.$$

Reordering the summations in the rightmost term of this expression, we see

$$\sum_{a=1}^{d}\left(\sum_{i=1}^{d-1}\eta_i|U_{ii}^{(a)}|\right)^2=\sum_{i=1}^{d-1}\sum_{j=1}^{d-1}\eta_i\eta_j\left(\sum_{a=1}^{d}|U_{ii}^{(a)}||U_{jj}^{(a)}|\right).$$

Let $q\geq 1$ be the value of i that maximizes $\Sigma_{a=1}^{d}|U_{ii}^{(a)}|^2$ for $1\leq i\leq d-1$; then

$$\sum_{a=1}^{d}|U_{ii}^{(a)}||U_{jj}^{(a)}|\leq\frac{1}{2}\sum_{a=1}^{d}(|U_{ii}^{(a)}|^2+|U_{jj}^{(a)}|^2)\leq\sum_{a=1}^{d}|U_{qq}^{(a)}|^2,$$

which leads to

$$\sum_{a=0}^{d}|U_{00}^{(a)}|^2\leq 1+R_q\sum_{i=1}^{d-1}\sum_{j=1}^{d-1}\eta_i\eta_j=1+\eta^2R_q, \qquad (4.2)$$

where we have defined

$$\eta\equiv\sum_{i=1}^{d-1}\eta_i=\frac{1-\lambda_0}{\lambda_0},\quad R_q\equiv\sum_{a=1}^{d}|U_{qq}^{(a)}|^2.$$

Using $U^{(0)}=I$ and the fact that the length of each row of $U^{(a)}$ is one, we have

$$\sum_{a=0}^{d}|U_{q0}^{(a)}|^2=\sum_{a=1}^{d}|U_{q0}^{(a)}|^2=\sum_{a=1}^{d}\left(1-\sum_{k=1}^{d-1}|U_{qk}^{(a)}|^2\right)\leq d-R_q.$$

Normalization of the $(q0)$-th row of M allows the previous equation to be transformed into

$$1-\sum_{b=d+1}^{d^2-1}|\phi_{q0}^{(b)}|^2=\lambda_0\sum_{a=0}^{d}|U_{q0}^{(a)}|^2\leq\lambda_0(d-R_q). \qquad (4.3)$$

From Eq. (4.2),

$$R_q\geq\frac{\sum_{a=0}^{d}|U_{00}^{(a)}|^2-1}{\eta^2},$$

which along with the normalization of the (00)-th row of M,

$$\lambda_0\sum_{a=0}^{d}|U_{00}^{(a)}|^2+\sum_{b=d+1}^{d^2-1}|\phi_{00}^{(b)}|^2=1,$$

yields

$$R_q\geq\frac{1-\lambda_0-\sum_{b=d+1}^{d^2-1}|\phi_{00}^{(b)}|^2}{\lambda_0\eta^2}. \qquad (4.4)$$

Combining this with Eq. (4.3) gives

$$1-\sum_{b=d+1}^{d^2-1}|\phi_{q0}^{(b)}|^2\leq\lambda_0\left(d-\frac{1-\lambda_0-\sum_{b=d+1}^{d^2-1}|\phi_{00}^{(b)}|^2}{\lambda_0\eta^2}\right),$$

and thus

$$1-d\lambda_0+\frac{\lambda_0^2}{1-\lambda_0}\leq\sum_{b=d+1}^{d^2-1}|\phi_{q0}^{(b)}|^2+\frac{\lambda_0^2}{(1-\lambda_0)^2}\sum_{b=d+1}^{d^2-1}|\phi_{00}^{(b)}|^2. \qquad (4.5)$$

Applying Eq. (1.7) with $j=0$ and $K=d+1$, we obtain

$$\sum_{b=d+1}^{d^2-1}\sum_{k=0}^{d-1}|\phi_{k0}^{(b)}|^2=d-(d+1)\lambda_0. \qquad (4.6)$$

Equation (4.6) along with Eq. (4.5) yields the following sequence of inequalities:

$$1-d\lambda_0+\frac{\lambda_0^2}{1-\lambda_0}\leq\sum_{b=d+1}^{d^2-1}|\phi_{q0}^{(b)}|^2+\frac{\lambda_0^2}{(1-\lambda_0)^2}\Bigg[d-(d+1)\lambda_0-\sum_{b=d+1}^{d^2-1}\sum_{k=1}^{d-1}|\phi_{k0}^{(b)}|^2\Bigg]\leq\sum_{b=d+1}^{d^2-1}|\phi_{q0}^{(b)}|^2\left(1-\frac{\lambda_0^2}{(1-\lambda_0)^2}\right)+[d-(d+1)\lambda_0]\frac{\lambda_0^2}{(1-\lambda_0)^2}, \tag{4.7}$$

where to obtain Eq. (4.7), we have used $\Sigma_{k=1}^{d-1}|\phi_{k0}^{(b)}|^2\geq|\phi_{q0}^{(b)}|^2$, which is obvious since $q\geq 1$. Note that in the region of interest $\lambda_0>1/2$, the term $1-\frac{\lambda_0^2}{(1-\lambda_0)^2}$ will be negative; thus we maximize the right-hand side of the last inequality by inserting the smallest possible value of $\Sigma_b|\phi_{q0}^{(b)}|^2$, which is zero, leading to

$$1-d\lambda_0+\frac{\lambda_0^2}{1-\lambda_0}\leq[d-(d+1)\lambda_0]\frac{\lambda_0^2}{(1-\lambda_0)^2}.$$

Solving for λ_0 produces

$$\lambda_0\leq\frac{1}{2}\left(1+\sqrt{\frac{d-2}{d+2}}\right), \tag{4.8}$$

which is strictly less than the WCSG bound of $d/(d+1)$ for $d>2$. For $d=3$, it gives ≈ 0.7236, less than the WCSG bound of 3/4, but only about one third of the way toward the 2/3 bound conjectured by Mozes *et al.*

It might be thought that even when K is not restricted to the value $K=d+1$, an argument similar to the one just given also would push down—toward smaller values of λ_0—the WCSG bound $\lambda_0\leq d/K$. Saturation has been demonstrated in [6] for the WCSG bound for $K=d+2$ and $K=2d-1$. Generalization of the argument of this section for other K values is easily constructed but shows that an improvement in the WCSG bound comes only for the case $K=d+1$ shown above.

V. EXTENSION RESULTS IN CASE $K=d+1$

In Sec. IV, we established that when $K=d+1$, the WCSG bound $\lambda_0\leq d/(d+1)$ can be reduced to the value given in Eq. (4.8). However, as we have indicated, Mozes *et al.* [2] conjectured that this bound can be further reduced to $(d-1)/d$; moreover, they constructed for every d a family of $d+1$ encoding unitaries when $\lambda_0=(d-1)/d$. These families of $d+1$ encoding unitaries include both the identity operator I and the shift operator X defined by

$$X|j\rangle\equiv|j+1\rangle, j=0,1,2,\ldots,d-1, \text{ where } |d\rangle\equiv|0\rangle.$$

In this section, we show that whenever there is a family of $d+1$ encoding unitaries that includes I and X, then $\lambda_0\leq(d-1)/d$, in agreement with Mozes and coauthors' conjecture. We also obtain a more general bound on λ_0 in cases where an encoding family of unitaries includes not only I and X but additional powers of X.

We again address the d-dimensional dense-coding problem, with $K=d+1$. We seek the conditions under which we can have a set of $d+1$ encoding unitaries $\{U^{(a)}\}_{a=0}^{d}$ that include both the identity $I\equiv U^{(0)}$ and $X\equiv U^{(1)}$. Note that any set of encoding unitaries can be transformed so as to include I (see, e.g., [6], Lemma 2.1). It is obvious from the argument demonstrating this lemma, however, that any set of encoding unitaries also can be transformed to include X or indeed to include any other selected unitary whatsoever. Customarily, one assumes that the set of encoding unitaries has been transformed to include I; with this understanding assuming that the set also includes X makes the set special. Thus it perhaps is not surprising that for this special case, the Eq. (4.8) bound, which applies to all sets of $K=d+1$ unitaries, can be further reduced.

For the remaining $d-1$ unitaries $\{U^{(a)}\}_{a=2}^{d}$, their Λ orthogonality with the identity requires

$$U_{00}^{(a)}=-\sum_{j=1}^{d-1}\eta_jU_{jj}^{(a)} \tag{5.1}$$

and their Λ orthogonality with X requires

$$U_{10}^{(a)}=-\sum_{j=1}^{d-1}\eta_jU_{(j+1)j}^{(a)}, \tag{5.2}$$

recalling the definition $\eta_j\equiv\lambda_j/\lambda_0$. (Indices for matrix elements of $U^{(a)}$'s should be interpreted as integers modulo d; thus a term like $U_{d,d-1}^{(a)}$ should be identified with $U_{0,d-1}^{(a)}$.) Unitarity of each $U^{(a)}(a>1)$ allows us to write

$$\sum_{j=2}^{d-1}|U_{j0}^{(a)}|^2=1-|U_{00}^{(a)}|^2-|U_{10}^{(a)}|^2=1-\left|\sum_{j=1}^{d-1}\eta_jU_{jj}^{(a)}\right|^2-\left|\sum_{j=1}^{d-1}\eta_jU_{(j+1)j}^{(a)}\right|^2.$$

For $a\in\{2,3,\ldots,d\}$ and $j\in\{2,3,\ldots,d-1\}$, let $v_j^{(a)}$ be the two-dimensional vector whose first component is $U_{jj}^{(a)}$ and second is $U_{(j+1)j}^{(a)}$, with length $\|v_j^{(a)}\|\leq 1$ since this vector consists of two components of one of the columns of the unitary matrix $U^{(a)}$. We then can re-express the previous equation as

$$\sum_{j=2}^{d-1}|U_{j0}^{(a)}|^2=1-\left\|\sum_{j=1}^{d-1}\eta_jv_j^{(a)}\right\|^2\geq 1-\left(\sum_{j=1}^{d-1}\eta_j\|v_j^{(a)}\|\right)^2\geq 1-\left(\sum_{j=1}^{d-1}\eta_j\right)^2=1-\eta^2, \tag{5.3}$$

where we have used the triangle inequality to establish the second line in Eq. (5.3), and used $\eta\equiv\Sigma_{j=1}^{d}\eta_j=(1-\lambda_0)/\lambda_0$ in the final step.

Starting with Eq. (1.6), setting $j=j'=0$, $i'=i$, and summing over i from 2 to d-1 produces

$$d-2=\lambda_0\sum_{a=0}^{d}\sum_{i=2}^{d-1}|U_{i0}^{(a)}|^2+\sum_{b=d+1}^{d^2-1}\sum_{i=2}^{d-1}|\phi_{i0}^{(b)}|^2.$$

The $a=0$ and $a=1$ terms in the first sum are both zero, therefore [using Eq. (5.3)]

$$d-2 \geq \lambda_0 \sum_{a=2}^{d} \sum_{i=2}^{d-1} |U_{i0}^{(a)}|^2 \geq \lambda_0 (d-1)(1-\eta^2)$$

and consequently, $\lambda_0 \leq (d-1)/d$. Thus, the inclusion of both I and X as encoding unitaries in the $K=d+1$ case leads to the upper bound on λ_0 as postulated by Mozes *et al.* for the more general case.

Remarks:

(a) The argument presented above is easily modified to show that if a family of $d+1$ encoding unitaries contains both I and X^j for some $j \in \{1,2,\ldots,d-1\}$ then $\lambda_0 \leq (d-1)/d$. Note that if an encoding family $\{U^{(a)}\}$ contains any two operators from $\{X^k\}_{k=0}^{d-1}$, say $U^{(0)}=X^n$ and $U^{(1)}=X^m$, where $n>m$, then $\{X^{d-n}U^{(a)}\}$ will be an encoding family as well: one that includes I and X^j, where $j=d-n+m$. Thus, $\lambda_0 \leq (d-1)/d$ whenever there is an encoding family of $d+1$ unitaries containing any two (distinct) elements from $\{X^k\}_{k=0}^{d-1}$.

(b) A more careful analysis of the inequalities we have used in Eq. (5.3) to derive the bound $\lambda_0 \leq (d-1)/d$ leads to the following improvement. If there exists a Λ-orthogonal family of $d+1$ encoding unitaries including both I and X and if $\lambda_2>0$, then $\lambda_0<(d-1)/d$, an inequality also consistent with numerical results obtained by Mozes *et al.*

The method described in this section is quite general and can quickly be adapted to produce a more general result. Assume that I and $m-1$ additional powers of X are the first m encoding unitaries in the family $\{U^{(a)}\}_{a=0}^{K-1}$; that is, $U^{(a)}=X^a$ for $a=0,\ldots,m-1$ where $m\geq 1$, $d\geq m$, and $d+1\leq K\leq d^2$. There will be m expressions of the form of Eqs. (5.1) and (5.2) that simply lead to a generalization of Eq. (5.3),

$$\sum_{j=m}^{d-1} |U_{j0}^{(a)}|^2 \geq 1-\eta^2.$$

The key equation of the augmented message-matrix approach [Eq. (1.6)] with $j=j'=0$, $i'=i$, and summed over i from m to $d-1$ produces

$$d-m \geq \lambda_0 (K-m)(1-\eta^2)$$

leading to

$$\lambda_0 \leq \frac{K-m}{2K-m-d}. \tag{5.4}$$

Since $m\leq d$, the limit given on the right-hand side of Eq. (5.4) is no less than 1/2. It can therefore not produce a useful stricter limit than the WCSG bound of d/K unless $d/K \geq 1/2$, thus $K\leq 2d$. Also, when $m=1$, Eq. (5.4) never offers any improvement on the WCSG bound, which is not at all surprising since the assumption that $m=1$ is simply that the collection of encoding unitaries includes I.

Examples utilizing Eq. (5.4) include:

(a) if $m=2$ and $K=d+1$, we reproduce the result proved above, i.e., $\lambda_0 \leq (d-1)/d$,

(b) if $m=3$, $d=4$, and $K=5$, then $\lambda_0 \leq 2/3$, and

(c) if $m=2$ and $K=d+2$, we get $\lambda_0 \leq d/(d+2)$.

It is also noteworthy that if $m=d$ then $\lambda_0 \leq 1/2$ proving by an entirely different method Proposition 2.2 from our previous work [6].

A systematic but tedious utilization of length relationships resulting from the unitarity properties of the augmented message matrix and the $U^{(a)}$'s can produce a more restrictive bound for the case $m=2$ and $K=d+2$, under the additional requirements that $d=3$ and $\lambda_2=0$. The result is the expression

$$2(1-\eta) - \frac{\eta^3}{1-\eta^2} \leq 0,$$

yielding $\eta \leq \approx 0.68889$. Thus, while $K=5$ solutions can be found generally for values of $\lambda_0 \leq 3/5$ ($\eta \geq 2/3$) ([6], Proposition 3.5) this shows that if both I and X are included as encoding unitaries, a more restrictive limit applies, namely, $\lambda_0 \leq \approx 0.5921$. Paralleling this process, there is likely to be a variety of other restrictive limits that can be established.

VI. CONCLUSION

Herein we have shown the augmented message matrix to be a useful tool for the study of the standard two-party deterministic dense-coding protocol. It yields a uniform and simplified method of derivation of several interesting previously proved theorems: a theorem of Wu *et al.* introducing the WCSG bounds [4], which give an upper limit on the largest Schmidt coefficient $\sqrt{\lambda_0}$ of an entangled state that permits the communication of $K>d$ perfectly distinguishable messages ($\lambda_0 \leq d/K$); a theorem of Ji *et al.* [3] which establishes the impossibility of transmission of d^2-1 perfectly distinguishable messages with any pair of qudits not fully entangled; and a theorem of Beran and Cohen [7] which provides conditions ensuring that certain WCSG bounds are not saturated. Moreover, we have used the augmented message matrix to obtain a number of additional dense-coding results. In particular, we have shown that in order to send $d+1$ messages with one qudit from a partially entangled pair, the largest Schmidt coefficient $\sqrt{\lambda_0}$ of the state vector for the entangled pair must satisfy $\lambda_0 \leq 1/2[1+\sqrt{(d-2)/(d+2)}]$; a bound that is strictly less than the WCSG bound for this case, $d/(d+1)$. We have also established bounds on the largest Schmidt coefficient in cases where the encoding unitaries include, along with the identity operator I, the shift operator X, as well as higher powers of the shift operator.

Our approach has not fully yielded the conjectured bound of Ref. [2], $\lambda_0 \leq (d-1)/d$ when $K=d+1$, a conjecture very strongly supported by numerical computations in that work. It is likely that stronger inequalities than those generated in our Sec. IV can be found; thus further work along these lines seems very worthwhile. Moreover, although in general our approach is not expected to be useful when too many of the wave functions Alice generates are not mutually orthogonal, as can occur in so-called unambiguous dense coding [4], it is conceivable that our approach will continue to yield useful results when the number of nonorthogonal wave functions is small. For instance, we recommend our approach in the investigation of Beran and Cohen's conjecture [7] that—even in deterministic dense coding—for some sets of Schmidt coefficients Alice may be able to send more messages if some nonunitary coding is permitted. Another related open question of considerable interest (suggested to us by Cohen) is whether the impossibility of only d^2-1 messages remains true when one of the messages can be generated via a nonunitary operation, in particular, when one permits d^2-2 unitary messages to be supplemented by a single additional message created using Kraus operators [8].

ACKNOWLEDGMENTS

The authors are indebted to Scott Cohen, Robert Griffiths, and Frank Tabakin for useful discussions.

[1] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[2] S. Mozes, J. Oppenheim, and B. Reznik, Phys. Rev. A **71**, 012311 (2005).
[3] Z. Ji, Y. Feng, R. Duan, and M. Ying, Phys. Rev. A **73**, 034307 (2006).
[4] S. Wu, S. M. Cohen, Y. Sun, and R. B. Griffiths, Phys. Rev. A **73**, 042311 (2006).
[5] R. F. Werner, J. Phys. A **34**, 7081 (2001).
[6] P. S. Bourdon, E. Gerjuoy, J. P. McDonald, and H. T. Williams, Phys. Rev. A **77**, 022305 (2008).
[7] M. R. Beran and S. M. Cohen, Phys. Rev. A **79**, 032307 (2009).
[8] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).